CONNECTING BUSINESS & TECHNOLOGY

Séminaire de sensibilisation

LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

amadeus

02 et 03/03/2016

devoteam
Management Consulting

Sommaire

- Enjeux de la sécurité de l'information
- La cybercriminalité
- Résultats de l'audit des agences
- Consignes à respecter
- Quiz en sécurité de l'information

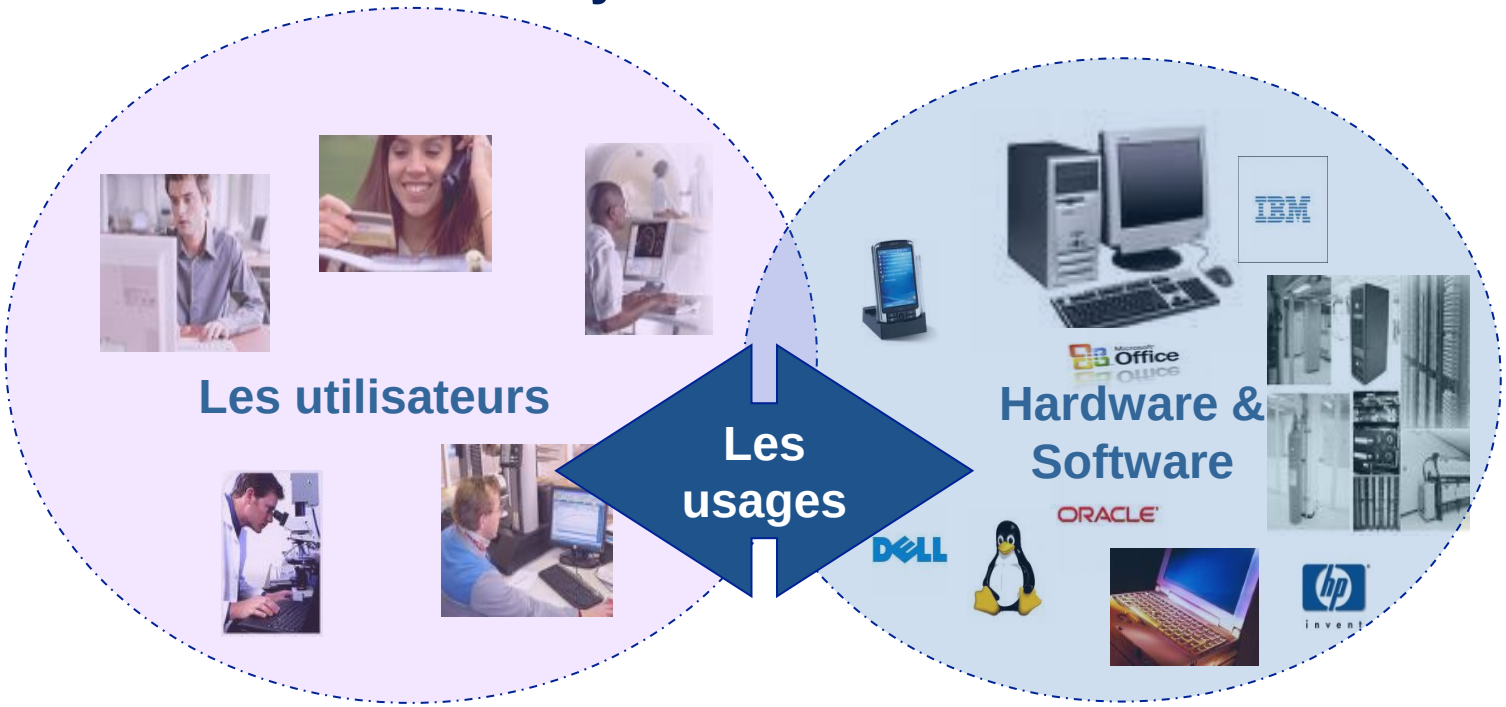
Contexte du séminaire

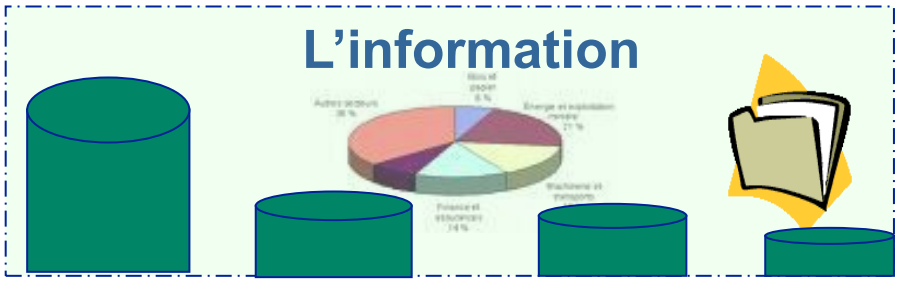
Opérant dans un environnement de plus en plus ouvert et confronté à une augmentation de menaces de toute nature pouvant impacter la sécurité de l'information, Amadeus a entamé des actions sur la sécurité de son patrimoine humain, informationnel et matériel.

Dans ce contexte, et afin de poursuivre les démarches déjà engagées, Amadeus a décidé de mener une **action de sensibilisation à l'ensemble des acteurs et des collaborateurs**, en y mettant en valeur les rôles qu'ils ont à jouer dans la protection du système d'information d'Amadeus.

Que faut il sécuriser?

Le système d'information





Enjeux de la sécurité

Les critères de la sécurité de l'information

- **Confidentialité:**

  L'information ne doit pas être divulguée à toute personne, entité ou processus non autorisé.

- **Intégrité:**

  Le caractère correct et complet des actifs doit être préservé. L'information ne peut être modifiée que par ceux qui en ont le droit.

- **Disponibilité:**

  L'information doit être rendue accessible et utilisable sur demande par une entité autorisée.

- **Traçabilité:**

  Tous les éléments liés à l'audibilité et à la preuve des transactions : Z a consulté l'information X à Y le jour J.

Les menaces existent…

Humaine

Intentionnelle

Externe

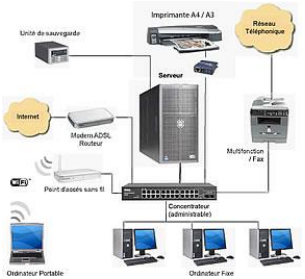
Interne

Piratage
Sabotage
Vol

Non intentionnelle

Personnel insuffisamment qualifié
Erreur humaine

Matérielle



Panne matériel

Coupure électrique

Incendie

Dysfonctionnement matériel ou logiciel

Naturelle

Activité géologique

Conditions météorologiques

…et les menaces évoluent

- L'évolution des menaces est liée à **la transformation des systèmes d'information** (et des réglementations).
- La menace concerne essentiellement **la malveillance** (menaces d'origine humaine et intentionnelle).
- Quatre profils sont généralement définis :

Catégorie 01	Catégorie 02	Catégorie 03	Catégorie 04
Ludique	**Cupide**	**Terroriste**	**Stratégique**
Sans profit	Pouvoir Argent	Idéologique	Economique Politique

- Quatre sources de risque:

Interne		Externe	
Accidentel	**Volontaire**	**Accidentel**	**Délibéré**

Cybercriminalité

- Une activité (profitable)
  - Plusieurs milliards de dollars de « chiffre d'affaires », équivalent aux revenus de la drogue.
  - Janvier 2014 : 800.000 euros détournés d'une banque suédoise par des pirates russes.
  - Juin 2015 : 4,74 millions de dollars détournés par des pirates brésiliens.
  - Une activité peu risquée
- Seuls 5% des auteurs d'infraction sont arrêtés et condamnés.
  - Identification difficile des personnes physiques impliquées.
- Les auteurs « bénéficient » de la diversité des lois anti cybercriminalité.
- Absence d'une législation homogène
- Une activité techniquement simple
  - Très souvent les outils sont disponibles gratuitement sur Internet.
  - Certains groupes de pirates revendent des kits « Clefs en main ».

Motivation

- **Cheval de Troie ou virus :** 1.000 / 5.000 $ en fonction de la complexité
- **Numéro de carte de crédit avec code PIN :** 500 $
- **Compte PayPal valide avec son mot de passe :** 7 $
- **Vulnérabilité dans Yahoo! Messenger :** 2.000 $
- **Attaque DDoS :** 500 $ / 1.500 $ par jour

- Sources :

  Finjan, TrendMicro, WebSense, MacAfee, Symantec

Sécurité des agences de voyage

Périmètre

Réalisation d'un audit de sécurité sur un échantillon de 12 agences entre Casablanca et Rabat.

Démarche

Réalisation de visites sur site → Réalisation d'entretiens avec les responsable → Elaboration du rapport

- Gestion du parc des postes de travail
- Gestion de l'accès internet
- Gestion des serveurs
- Gestion des utilisateurs
- Sécurité des smartphones
- Sécurité physique

Référentiels

- Bonnes pratiques de sécurité physique, organisationnelle et technique

Référentiel de notation des agences

	[0-1]	[2,3]	4	5
Maturité	**Sommeil**	**Eveil**	**Croissance**	**Maturité**
Gestion des utilisateurs	Agence non sensibilisée à la sécurité	Des consignes de sécurité sont communiquées au personnel, mais sans réel suivi de la direction/entité SI	Des consignes de sécurité sont communiquées au personnel et la direction/entité SI veille au respect des consignes	La sécurité est dans la culture de l'agence
Gestion des postes de travail et des smartphones	Parc obsolète (système d'exploitation XP, antivirus expiré ou non installé, etc.)	Mesures rudimentaires Postes de travail et smartphones sécurisés par des mots de passe et/ou avec un antivirus activé	Le parc informatique est sécurisé , à jour et contrôlé régulièrement	Postes de travail adhérents à un contrôleur de domaine maitrisé
Continuité d'activité	Agence non sensibilisée	Absence d'une stratégie de sauvegarde de données bien définie	Un plan de continuité d'activité est élaboré	Le plan d'activité est actualisé régulièrement
Gestion de l'accès internet	Le réseau de l'agence est non sécurisé (Un seul accès filaire et wifi non sécurisé)	Une seule ligne internet avec accès en LAN et Wifi sécurisé WPA / WPA 2	- Accès internet uniquement avec câble Ethernet. - Réseau wifi séparé du réseau LAN en WPA2 non communiqué	Existence d'une séparation logique ou physique des accès à internet avec contrôle de flux
Sécurité physique	Aucune mesure de sécurité physique n'est déployée	Les mesures déployées sont rudimentaires	Existence de plusieurs mesures de sécurité physique	La sécurité physique est maîtrisée et optimisée

Référentiel de notation des agences

	[0-1]	[2,3]	4	5
Maturité	Sommeil	Eveil	Croissance	Maturité

Gestion des utilisateurs

Gestion des postes de travail et des smartphones

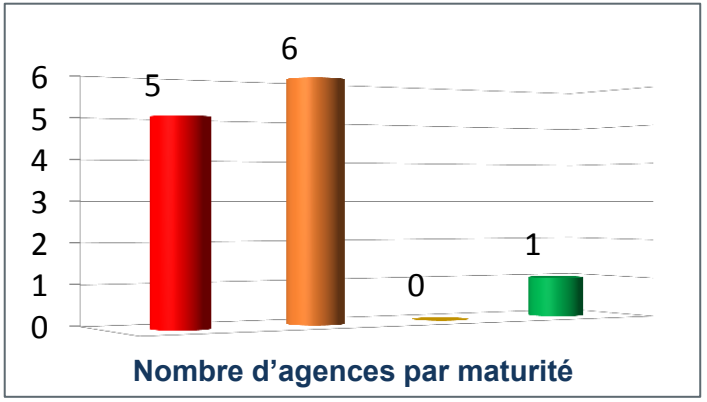
Continuité d'activité

Gestion de l'accès internet

Sécurité physique

Constats

- Les utilisateurs de l'agence ne sont pas sensibilisés par rapport à la sécurité du système d'information
- Les utilisateurs stockent leurs mots de passes applicatifs sur leurs navigateurs
- Les utilisateurs ne ferment pas leurs sessions avant de quitter leurs postes
- Les utilisateurs peuvent émettre des billets depuis leur propres postes de travail à domicile ;



Recommandations

- Instaurer des séances de sensibilisation périodique pour l'ensemble du personnel des agences sur les bonnes pratiques de la sécurité et lois et réglementations en vigueur Maroc relatifs à la sécurité de l'information
- Elaborer une charte d'utilisation des moyens informatiques et la faire signer par tout le personnel de l'agence
- Mettre en place une politique de gestion des mots de passe des utilisateurs
- Configurer les navigateurs internet à ne pas enregistrer les mots de passe

Référentiel de notation des agences

	[0-1]	[2,3]	4	5
Maturité	**Sommeil**	**Eveil**	**Croissance**	**Maturité**

Gestion des utilisateurs

Gestion des postes de travail et des smartphones

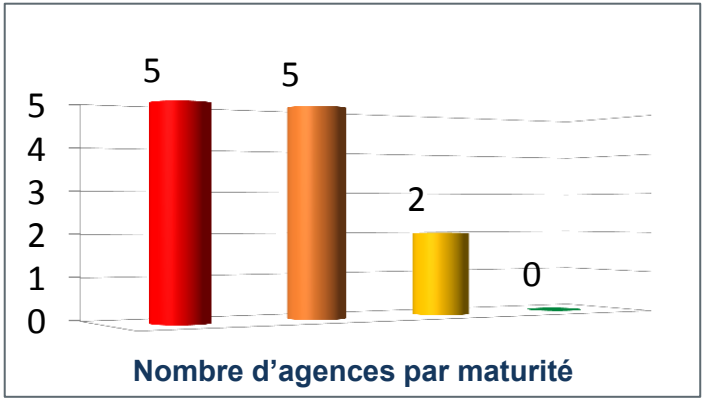
Continuité d'activité

Gestion de l'accès internet

Sécurité physique

Constats

- Plusieurs postes de travail tournent avec des systèmes d'exploitation obsolètes (Windows XP)
- Absence de solution antivirale
- Les utilisateurs ont le droit administrateur sur leurs postes
- Existence de solutions d'accès à distance installés sur les postes utilisateurs
- La Gestion des postes de travail et des smartphones n'est pas maitrisé en terme de mises à jour et de correctifs de sécurité
- La sécurité des smartphones n'est pas gérée au sein des agences



Recommandations

- Migrer tous les systèmes d'exploitation vers Windows 7
- Mettre en place une solution antivirale robuste
- Adopter la politique du moindre privilège dans la création des comptes utilisateur
- Faire adhérer tous les postes de travail dans un seul contrôleur de domaine afin contrôler la sécurité de tout le parc informatique

Référentiel de notation des agences

	[0-1]	[2,3]	4	5
Maturité	Sommeil	Eveil	Croissance	Maturité

Gestion des utilisateurs

Gestion des postes de travail et des smartphones

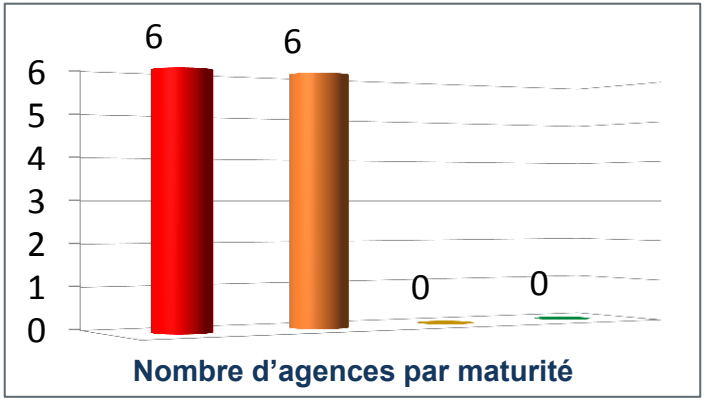
Continuité d'activité

Gestion de l'accès internet

Sécurité physique

Constats

- Existence de serveurs avec des systèmes d'exploitation obsolètes
- Absence de solution antivirale
- Installation de solution antivirale gratuite non à jour sur les serveurs
- Absence d'une politique de sauvegarde bien définie
- Les serveurs sont sur le même réseau que les utilisateurs



Recommandations

- Migrer tous les serveurs obsolètes vers des systèmes d'exploitation récents
- Déployer une solution antivirale robuste et veiller à sa mise à jour périodique
- Réaliser des sauvegardes périodiques des données selon un plan de sauvegarde bien défini
- Renforcer l'architecture réseau en séparant les serveurs et les utilisateurs via des VLANs

Référentiel de notation des agences

	[0-1]	[2,3]	4	5
Maturité	**Sommeil**	**Eveil**	**Croissance**	**Maturité**

Gestion des utilisateurs

Gestion des postes de travail et des smartphones

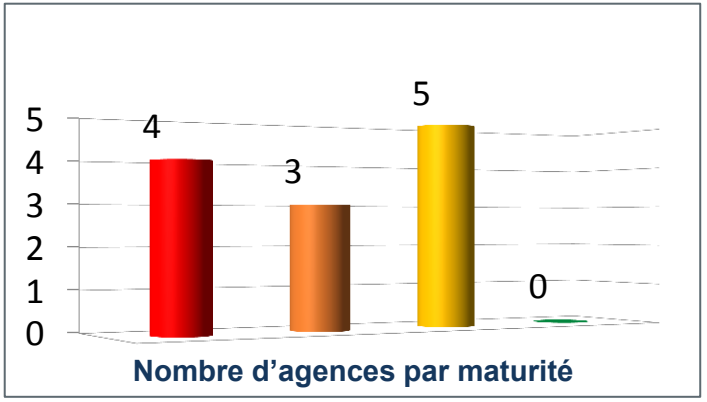
Continuité d'activité

Gestion de l'accès internet

Sécurité physique

Constats

- Plusieurs agences ont des accès Wifi avec un mot de passe de type WEP
- Plusieurs agences partagent les mots de passe Wifi avec leurs visiteurs et voisins
- L'accès au réseau Wifi donne accès au réseau local de l'agence
- Absence de filtrage web au niveau de certaines agences



Recommandations

- Mettre en place des mots de passe WPA2 sur les routeurs Wifi
- Désactiver ce type d'accès à internet si il est non nécessaire
- Mettre en place une connexion secondaire pour les visiteurs

Les bonnes pratiques pour la sécurité du poste de travail?

Quelles sont les menaces pour mon PC ?

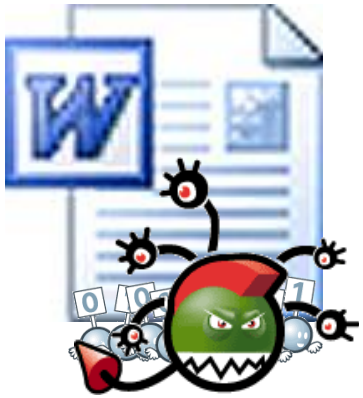
- **Menaces « aveugles »**
  - Virus
  - Ver(Worm)
  - Spam
  - …
- **Menaces ciblées**
  - Attaques ciblées en ligne
  - Divulgation par chat

Quelles sont les menaces pour mon PC ?

♦ Menaces «aveugles»

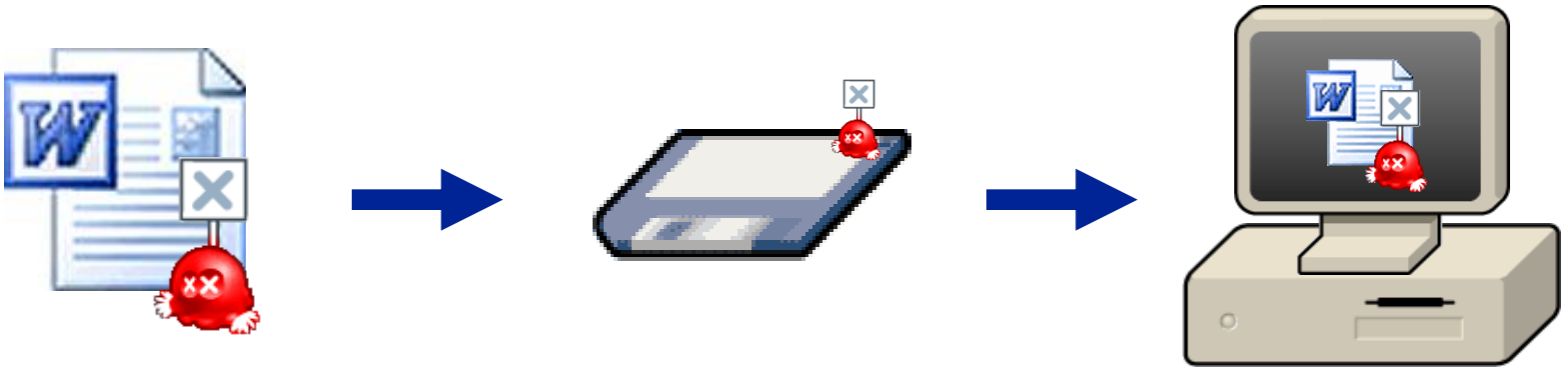
- ✓ Virus

Fichier word

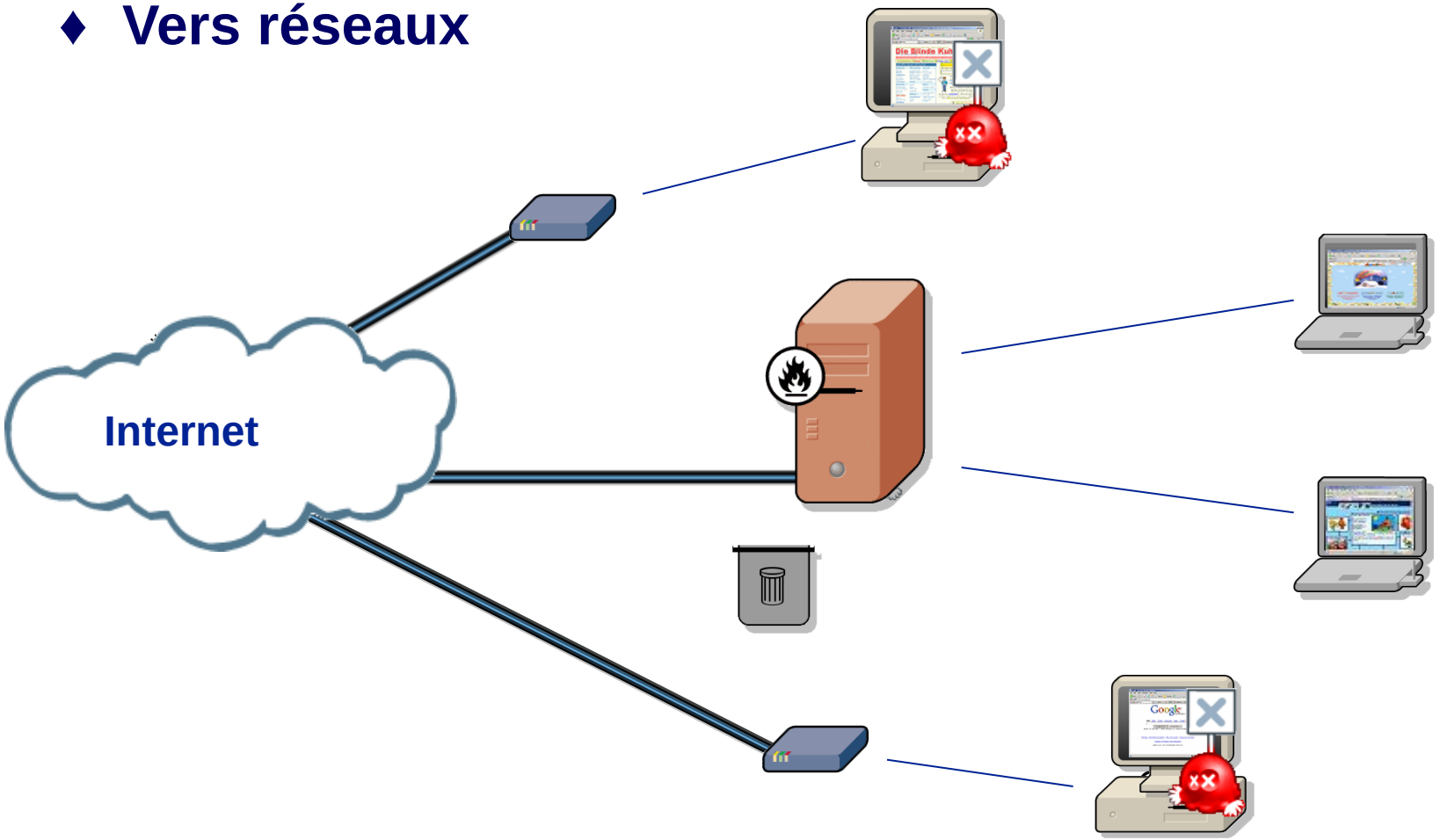


♦ Virus

- ❖ Un virus est un logiciel qui s'attache à tout type de document électronique, et dont le but est d'infecter ceux-ci et de se propager sur d'autres documents et d'autres ordinateurs.
- ❖ Un virus a besoin d'une intervention humaine pour se propager.

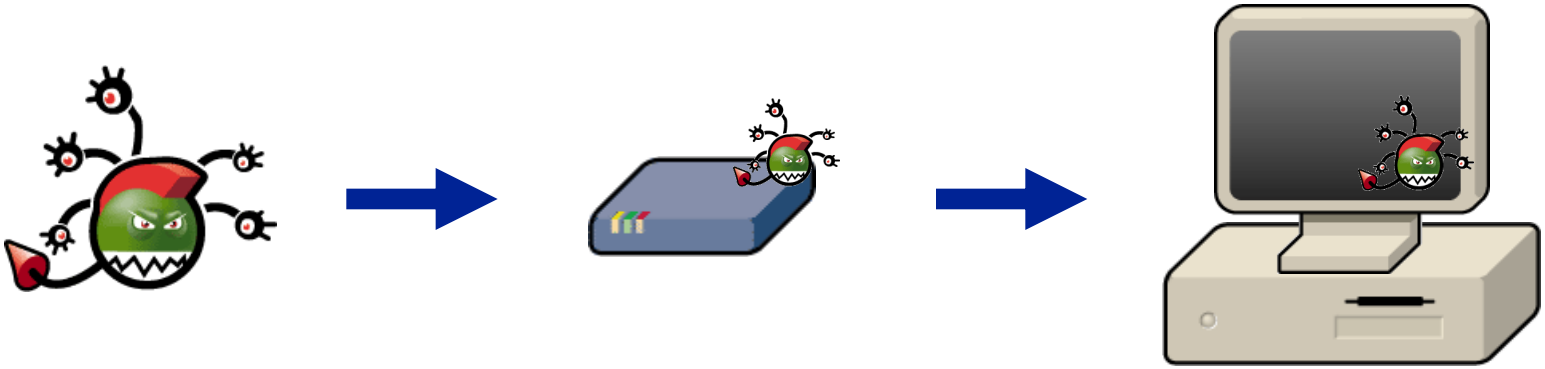


♦ Vers réseaux

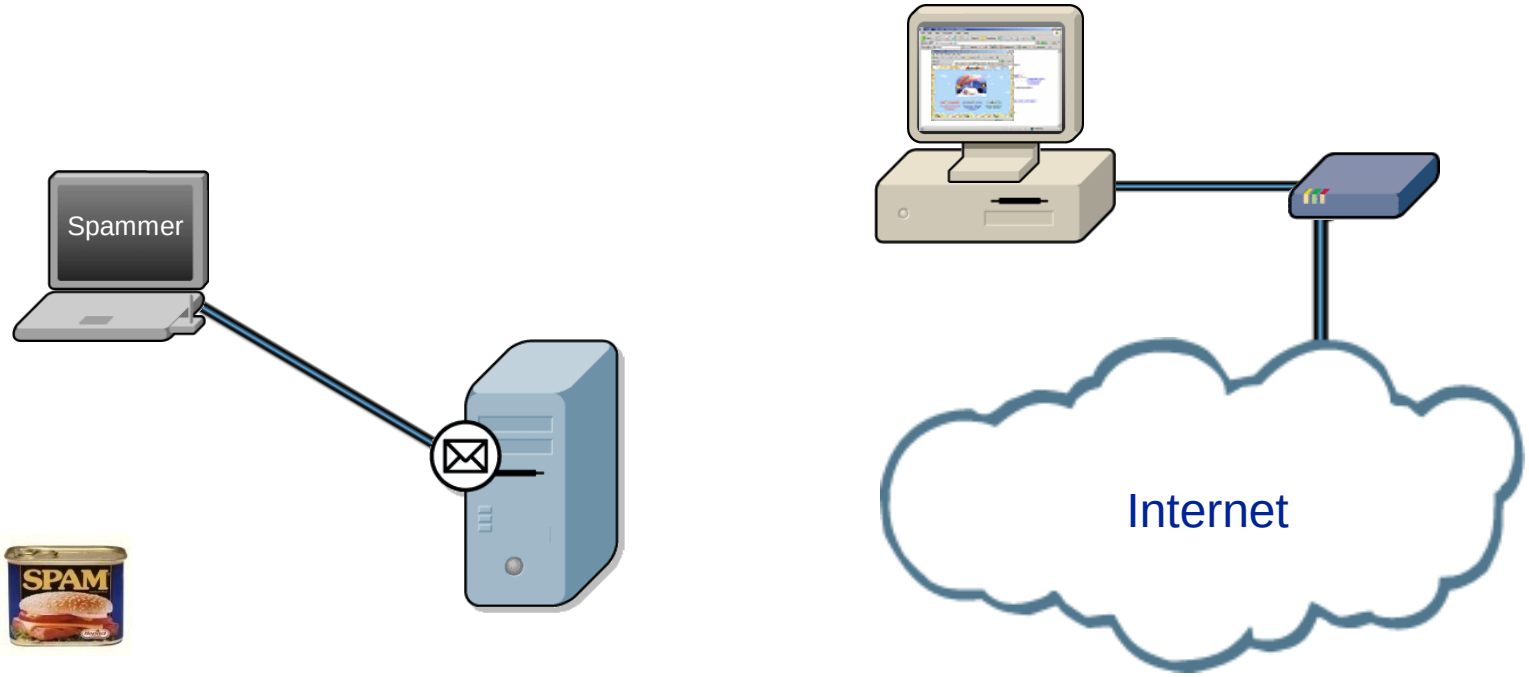


♦ Vers

- ✓ Un ver se reproduit en s'envoyant à travers un réseau (e-mail, Bluetooth, chat..)
- ✓ Le ver n'a pas besoin de l'interaction humaine pour pouvoir se proliférer.

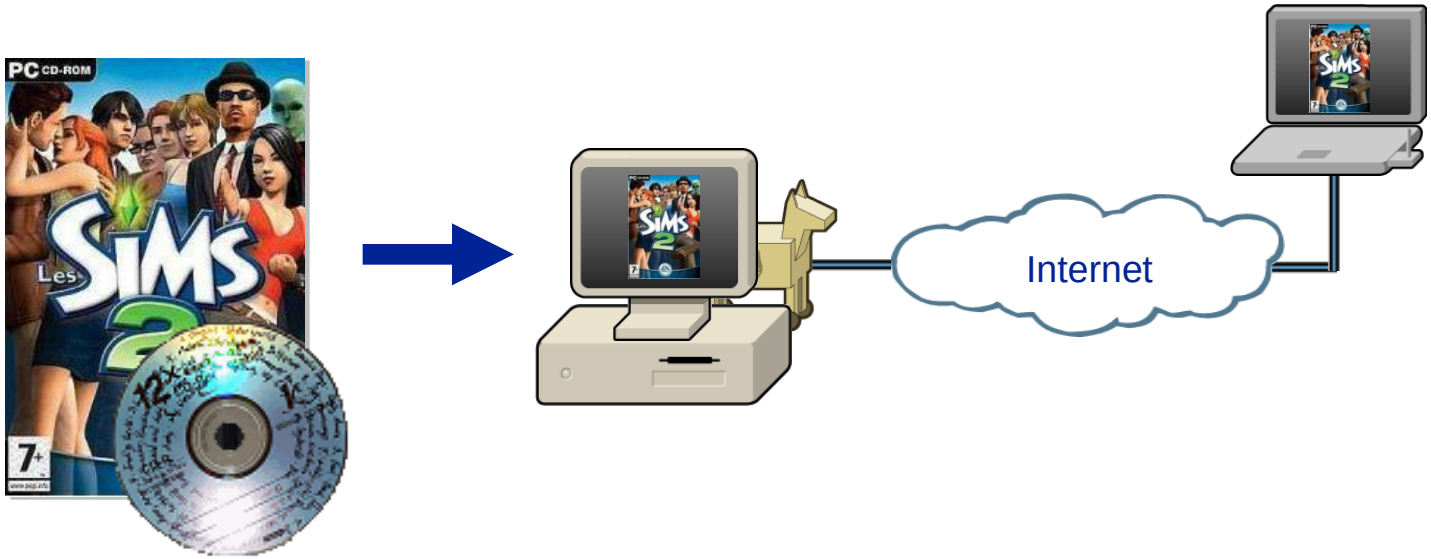


- **Spam**
  - ✓ **Le spam est du courrier électronique non sollicité envoyé a un très grand nombre de personnes sans leur accord préalable.**



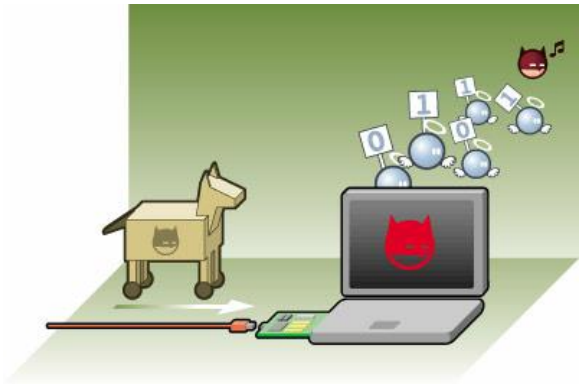
Quelles sont les menaces pour mon PC ?

- **Cheval de Troie**



Quelles sont les menaces pour mon PC ?

- **Cheval de Troie**
  - ✓ Programme bénin (jeux, documents…) cachant un autre programme.
  - ✓ Lorsque le programme est exécuté, le programme caché s'exécute aussi et pourrait ouvrir une « porte cachée ».
  - ✓ Contrôle du PC de l'extérieur



- **Conséquences de cette attaque**
  - ✓ perte de données
  - ✓ divulgation de données privées (chat, e-mails …)
  - ✓ espionnage: microphone, webcam
  - ✓ attaques à partir du PC « infecté »

Consignes à respecter

- Tout compte utilisateur ne doit pas avoir des privilèges administrateur;
- L'utilisateur ne doit pas installer des logiciels sur son ordinateur;
- L'utilisateur doit éviter de modifier la configuration du poste de travail;
- L'utilisateur doit effectuer des sauvegardes régulières des documents importants ;
- Le verrouillage du poste de travail à l'aide des écrans de veille automatique avec un mot de passe doit devenir une pratique courante.
- Ne jamais désactiver la solution antivirale et toujours veiller à sa mise à jour
- Ne jamais copier sur le poste de travail des fichiers provenant des clés USB douteuses ;

Comment sécuriser ma messagerie?

Consignes à respecter

- ☑ Vérifier la source des e-mails avant de les ouvrir, avant d'y répondre ou de les transmettre ;
- ☑ Ne jamais ouvrir les pièces jointes à des courriers électroniques dont l'expéditeur est inconnu. Tous les courriers électroniques suspects doivent être signaler;
- ☑ Ne jamais faire circuler des messages e-mails non professionnels (messages comportant des propos provocants ou à caractère injurieux, raciste, etc.) ;
- ☑ L'utilisateur est responsable de tout ce qui est écris dans son e-mail ;

Comment sécuriser mon mot de passe et ma session applicative?

Consignes à respecter

- Changer le mot de passe dès réception, et le modifier d'une façon périodique ne dépassant pas 3 mois;
- Ne jamais communiquer le mot de passe à une autre personne (Responsables, Collègues, ...) ;
- Toujours constituer des mots de passe complexes (minuscules, majuscules, chiffres, lettres, caractères spéciaux…) ;
- Ne jamais écrire le mot de passe sur un support papier à proximité du poste de travail.
- Toujours fermer la session applicative avant de quitter le poste
- Ne pas accéder à des modules applicatifs ou à des données métiers qui ne relèvent pas de vos attributions ;
- Ne pas divulguer des informations à des personnes non habilitées ;

Comment protéger les informations non numérisées ?

Consignes à respecter

❖*Toujours protéger les documents papiers contenant des informations confidentielles en les gardant dans des tiroirs fermés, coffres forts ou armoires ;*

❖*Broyer tout document confidentiel non nécessaire;*

❖*Protéger les médias de sauvegarde en les gardant dans un emplacement sécurisé (coffre ignifuge, armoire fermée à clé) ;*

❖*Veiller à l'archivage adéquat des documents et des informations sensibles.*

❖*Utiliser des chemises-bulles avec des codes couleur pour marquer la sensibilité des documents*

Quelle est la réglementation en vigueur?

Consignes à respecter

La législation marocaine a instauré des lois qui traitent la sécurité de l'information ; notamment :

- ***Loi 07-03 :*** *complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données ;*
- ***Loi 53-05 :*** *relative à l'échange électronique de données juridiques ;*
- ***Loi 09-08 :*** *relative à la protection des données à caractères personnel.*
- ***Loi 02-00:*** *relative à la propriété intellectuelle*

Extrait de la loi 07-03 :

Le fait d'accéder, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un mois à trois mois d'emprisonnement et de 2.000 à 10.000 dirhams d'amende ou de l'une de ces deux peines seulement.

Extrait de la loi 09-08 :

On risque une amende de 10.000 à 100.000 dirhams, si on continue à mettre en œuvre un fichier de données à caractère personnel sans déclaration ou autorisation.

Quiz en sécurité de l'information

Quiz (1/4)

1. J’ai installé un antivirus, suis-je désormais protégé contre les virus?

a) Vrai
b) Faux

Faux, Ce n'est pas suffisant, vous devez vérifier que votre antivirus se connecte bien à Internet régulièrement pour vérifier la disponibilité de mises à jour.

2. Un employé d'Amadeus vous appelle et vous demande votre code confidentiel d’accès à vos comptes en ligne pour régler un problème technique. Que faites-vous?

a) Je lui donne mon mot de passe et lui demande de me prévenir quand le problème sera réglé
b) Je refuse de lui donner mon mot de passe
c) Je lui donne mais je lui demande son nom en cas de problème

Je refuse de lui donner mon mot de passe car aucun employé d'Amadeus n’a le droit ni même les membres de l’équipe informatique n’ont le droit de vous demandez votre code d’accès confidentiel

Quiz (2/4)

3. <u>Un pare-feu me protège-t-il des attaques en provenance d'Internet ?</u>

a) Vrai
b) Faux

Vrai, s'il est réglé correctement, un pare-feu évite que des pirates puissent accéder à votre machine depuis Internet

4. <u>Vous recevez un e-mail de Microsoft avec en pièce jointe une mise à jour de sécurité importante. Que faites-vous ?</u>

a) Comme cela vient de Microsoft, je l'installe immédiatement
b) Je vérifie que l'adresse e-mail se termine bien par « microsoft.com » avant d'ouvrir la pièce jointe
c) J'efface l'e-mail et je retourne à mes occupations

J'efface l'email et je retourne à mes occupations parce que ni Microsoft, ni aucun autre éditeur de logiciel n'envoie de mises à jour par e-mail, et ne prévient pas de la disponibilité de celles-ci. Ne cliquez pas sur les liens et n'ouvrez pas la pièce jointe.

Quiz (3/4)

5. <u>Je peux accéder sans danger à mes comptes en ligne depuis un cybercafé car la communication est sécurisée</u>

a) Vrai
b) Faux

Faux, même si la communication est sécurisée, vous ne savez pas si le PC du cybercafé contient des virus ou des chevaux de Troie. Or, certains de ces programmes enregistrent tout ce que vous saisissez sur le clavier, y compris vos codes confidentiels d'accès.

6. <u>Un ami très proche vous envoie par e-mail une petite application qu'il qualifie de « très amusante », que faîtes-vous ?</u>

a) Après avoir vérifié que c'est effectivement votre ami et non un virus qui vous a envoyé l'application, vous l'ouvrez pour regarder de quoi il s'agit
b) Vous pensez qu'il n'a pas forcément vérifié la source de cette application et qu'il l'a probablement reçue de quelqu'un d'autre. Vous vous absentez et attendez de passer chez lui pour voir de quoi il s'agit
c) Vous pensez que cela peut être un virus, mais confiant dans vos logiciels de sécurité Internet, vos ouvrez la pièce jointe.

Il est tout à fait déconseillé d'ouvrir ou d'installer un logiciel autre que ceux qui proviennent d'éditeurs connus. C'est un des moyens préférés des pirates pour distribuer des virus.

Quiz (4/4)

7. Quels sont les principaux facteurs de risque en sécurité informatique ?

a) Défaillance du matériel
b) Erreurs humaines et mauvais comportement
c) Les événements naturels
d) Panne d'électricité

Les principaux risques sont les erreurs humaines et le mauvais comportement.

8. Si je procède à des activités peu sûres sur mon ordinateur et que j'installe moi-même des logiciels, je suis le seul à courir un risque.

a) Vrai
b) Faux

Faux, toute l'agence de voyage est aussi concernée

9. De quoi est capable un virus informatique ?

a) Modifier le fonctionnement de votre ordinateur
b) Envoyer des messages électroniques frauduleux à partir de votre ordinateur
c) Bloquer le système de votre ordinateur et provoquer le redémarrage intempestifs
d) Toutes les réponses ci-dessus

La bonne réponse est: toutes les réponses ci-dessus

Séminaire de sensibilisation

MERCI DE VOTRE ATTENTION

LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

amadeus

devoteam
Management Consulting

amadeus

Guide de sécurité

CONNECTING BUSINESS & TECHNOLOGY

devoteam

Consulting • Solutions • Expertise

TABLE DES MATIERES

1 ETAT D'ART

Les ordinateurs, les logiciels et le matériel de télécommunications sont devenus des composants intégraux du poste de travail et des vecteurs primaires pour la communication professionnelle. Afin d'assurer le maximum d'efficacité, de productivité et de sécurité, les dispositions suivantes régissent l'utilisation des ressources de communication du personnel de l'agence de voyage.

Le présent guide est un code de conduite dont l'objet est de définir les conditions générales d'utilisation des outils informatiques et moyens de communication mis en œuvre par votre agence de voyage pour aider vos collaborateurs à réaliser leurs tâches et missions en toute sécurité. Ainsi, il répond ; aux besoins professionnels de service, le patrimoine informationnel et documentaire, le système d'information et l'infrastructure informatique et télécommunication.

2 PRINCIPES FONDAMENTAUX

Le système informatique (SI) permet aux utilisateurs d'accéder aux données nécessaires à l'accomplissement de leurs activités professionnelles alliant ainsi des objectifs de qualité, d'adaptabilité, de compétitivité, de rentabilité, d'universalité et de rapidité des échanges d'informations.

Ces informations constituent une ressource importante de l'agence de voyage au même titre que les ressources financières et matérielles.

2.1. OBJECTIF DU GUIDE DE SECURITE

Le présent guide, est avant tout un code de bonne conduite recensant les bonnes pratiques de sécurité du système d'information. Il a pour objectifs de :

- Sensibiliser et responsabiliser les collaborateurs, en faisant expressément mention de leurs droits et obligations quant aux modalités et conditions d'utilisation du système informatique sans faillir aux règles déontologiques prévalant en la matière et aux prescriptions règlementaires en vigueur.
- Protéger les collaborateurs et les données gérées par ceux-ci en minimisant les risques liés au mauvais usage du système informatique.

2.2. LOIS ET REGLEMENTATIONS EN VIGUEUR AU MAROC

Actuellement, il existe des lois et des réglementations en vigueur au Maroc relatifs à la sécurité de l'information, auxquelles tout utilisateur doit s'y conformer. Les lois en question sont présentées dans ce qui suit à titre énonciatif et non limitatif :

- **Loi 07-03 :** complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données publiée au Bulletin Officiel n° 5184 du 5 février 2004 ;
- **Loi 53-05 :** relative à l'échange électronique de données juridiques qui précise les règles liées à l'utilisation de moyens cryptographiques pour l'échange de données ;

- **Loi 09-08 :** relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel publiée au Bulletin Officiel n° 5744 du 18 Juin 2009 ;
- **La loi n°2-00 :** portant promulgation relative aux droits d'auteur et droits voisins.

2.3. DÉFINITION

- **Utilisateur** : Il s'agit de toute personne ayant accès dans le cadre de l'exercice de son activité professionnelle au système informatique, quel que soit son statut, notamment :
  - Les collaborateurs,
  - Les stagiaires externes,
  - Le personnel des prestataires de services intervenant sur les sites appartenant à l'Agence de voyage.
- **Système informatique** : Ensemble des ressources techniques requises par le traitement des informations. Il comporte tous les matériels informatiques et réseaux, équipements périphériques, logiciels et applications dont l'agence de voyage est propriétaire ou gestionnaire, ou qui sont utilisés dans ses locaux.

3.1. UTILISATION PROFESSIONNELLE

Chaque utilisateur ayant un droit d'accès au système informatique est censé avoir pris acte de son engagement à l'utiliser dans un cadre professionnel. Autrement dit, les utilisations personnelles, sont à cet égard prohibées, sauf autorisation préalable. Il est également prohibé le recours à des procédés pouvant servir directement ou indirectement des intérêts personnels de l'utilisateur, susceptibles de mettre en cause ou compromettre la bonne utilisation du système.

3.2. SÉCURITÉ

La sécurité du SI est l'affaire de tous et doit avoir la priorité et l'importance requises.

Tout utilisateur est responsable de la sécurité des ressources qui lui sont affectées. A cette fin, il s'engage à observer les règles suivantes :

- Contribuer dans la mesure du possible à la vérification de l'installation de l'antivirus sur son poste et à effectuer les mises à jours de sécurité,
- Veiller à accéder à partir de l'infrastructure de l'agence de voyage vers l'extérieur via les dispositifs sécurisés mis en place. La connexion et l'installation de moyen de télécommunication avec l'extérieur doit être agréée et contrôlée explicitement par l'entité SI.
- Solliciter l'appui et l'assistance de l'équipe technique pour toute installation de logiciel,
- Eviter de modifier la configuration du poste de travail et des équipements informatiques,

- Utiliser les fils de sécurité pour préserver l'intégrité physique des ordinateurs portables à l'intérieur ou à l'extérieur du lieu de travail,
- Sécuriser les Smartphones par des mots de passe,
- Analyser tout média amovible (CD, DVD, clés USB,…) avant son utilisation,
- Eviter d'ouvrir, de répondre ou de transférer les messages de types « SPAM » ou douteux qui n'ont pas pu être détectés et bloqués par le serveur de messagerie,
- Eviter de donner l'adresse mail professionnelle sur les sites internet non professionnels,
- Rapporter tout incident douteux à l'entité SI pour permettre le diagnostic du problème,
- Utiliser les systèmes informatiques d'une manière rationnelle afin d'éviter la saturation ou leur détournement à des fins personnelles,
- S'interdire d'accéder à des ressources diffusées au sein du système informatique pour lesquelles l'utilisateur ne bénéficie pas d'une habilitation ; l'utilisateur doit limiter ses accès aux seules ressources pour lesquelles il est expressément habilité à l'exclusion de toute autre, même si cet accès est techniquement possible,
- Veiller à la protection des données informatiques qu'il détient. Il lui appartient de protéger ces données en utilisant les différents moyens de sauvegarde mis à sa disposition,
- Se rendre responsable des droits d'accès attribués aux autres utilisateurs,
- Préserver la sécurité physique des moyens informatiques mis à sa disposition,
- Ne pas tenter de lire, modifier, copier ou détruire des données autres que celles autorisées,
- Ne pas utiliser les Wi-Fi « publics » (réseaux offerts dans les cafés, les gares, les aéroports ou les hôtels, etc.) pour des raisons de sécurité et de confidentialité
- Signaler toute tentative de violation de son compte et de façon générale, toute anomalie constatée,
- Choisir des mots de passe sûrs, gardés secrets et en aucun cas les communiquer à des tiers,
- S'engager à ne pas mettre à disposition d'utilisateurs non autorisés un accès aux systèmes ou au réseau à travers des matériels en sa possession.
- S'engager à, ne pas utiliser des comptes autres que le sien et ne pas masquer sa véritable identité.
- Veiller à ne pas propager de virus informatiques.

- Ne pas quitter son poste de travail sans le verrouiller en laissant des ressources ou des services accessibles.

3.3. DROIT D'ACCÈS

Chaque utilisateur reçoit un droit d'accès individuel qui se matérialise, le cas échéant, par tout moyen logique ou physique (tel que code d'accès, mot de passe, badge, …)

- L'utilisateur s'engage à ne jamais communiquer son mot de passe.
- Le droit d'accès est strictement personnel et incessible. Il cesse automatiquement lorsque l'utilisateur quitte l'agence de voyage,
- Le droit d'accès est conféré pour une utilisation conforme aux missions assignées. Toute autre utilisation est interdite,
- L'utilisateur doit protéger l'accès de son micro-ordinateur. Il doit fermer les sessions ouvertes à son nom avant de quitter les lieux et activer la mise en veille automatique protégée par un mot de passe après une courte période d'inactivité.
- Le mot de passe doit être unique pour chaque site/service,
- Le mot de passe de la messagerie professionnelle doit être différent de celui de la messagerie personnelle;
- Le mot de passe ne doit pas contenir des informations personnelles facilement devinables,
- L'utilisateur doit renouveler ses mots de passe avec une fréquence raisonnable ne dépassant pas 90 jours;
- L'utilisateur ne doit pas stocker les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur Internet), encore moins sur un papier facilement accessible (exemple : post-it) ;
- L'utilisateur ne doit pas envoyer ses propres mots de passe sur la messagerie;
- L'utilisateur doit veiller à ne pas enregistrer les mots de passe sur les navigateurs web.

3.4. CONFIDENTIALITÉ DES DONNÉES

La préservation des intérêts de votre agence de voyage nécessite le respect par tous d'une obligation générale et permanente de confidentialité, de discrétion et de secret professionnel à l'égard des informations et documents électroniques disponibles au sein du système informatique.

Le respect de cette confidentialité implique notamment de :

- Prendre toutes les mesures nécessaires afin de protéger la confidentialité des données,

- Veiller à sécuriser tout actif organisationnel (document papier, cd,..) propre à l'agence de voyage.
- D'une manière générale, respecter les règles de conscience professionnelle, de déontologie, ainsi que les obligations de réserve et devoir de discrétion en usage au sein de l'agence de voyage.

3.5. SAUVEGARDE DES DONNÉES

Les données stockées sur le serveur commun sont sauvegardées par l'entité SI et sont sous sa responsabilité. La fréquence de sauvegarde, la durée de rétention et la rotation des supports sont déterminés et affichées au niveau de la politique de sauvegarde.

- Les serveurs déployés dans les différentes entités doivent être sauvegardés par un collaborateur de l'entité.
- chaque utilisateur doit opérer les sauvegardes de ses données dans l'espace de stockage du serveur qui lui est attribué.
- Tous les documents sur lesquels vous travaillez doivent être ouverts, modifiés et enregistrés dans cet espace (même quand l'utilisateur est à l'extérieur de son bureau).
- L'utilisateur se doit d'isoler les fichiers et les messages important et veiller à les archiver pour pouvoir les retrouver en cas de défaillance de son poste de travail .

3.6. RESPECT DES DROITS DE LA PROPRIÉTÉ INTELLECTUELLE

Dans le but de respecter les droits de propriété intellectuelle des logiciels et des données, deux niveaux de restriction sont à observer :

- La direction se doit d'acquérir les droits et les agréments nécessaires des logiciels utilisés. Autrement dit, les utilisateurs ne peuvent installer des logiciels piratés, copiés, récupérés, modifiés.
- Les fichiers, les données et les informations contenus dans le système informatique de l'agence de voyage, sont sa propriété.

3.7. USAGE DE LA MESSAGERIE ET DES SERVICES INTERNET

- L'utilisateur doit faire usage de la messagerie et des services Internet dans le cadre de ses activités professionnelles en conformité avec la législation en vigueur. Il est responsable du contenu qu'il insère ou envoie par le biais de la messagerie électronique professionnelle, il se doit de :
- ne pas lire ou de prendre connaissance de tout message électronique appartenant ou destiné à un tiers
- se connecter au serveur de messagerie conformément aux dispositions prévues.

- éviter toute action mettant en péril la sécurité et le bon fonctionnement des serveurs
- s'interdire de s'approprier l'identité d'une autre personne ou intercepter des communications entre tiers,
- ne pas utiliser la messagerie ou les services internet pour proposer ou rendre accessible aux tiers des données et informations confidentielles ou contraires à la législation en vigueur,
- éviter de faire circuler des messages électroniques non professionnels ou portants atteinte à l'intégrité d'un autre utilisateur, notamment par des messages comportant des images provocantes ou à caractère injurieux et raciste, etc.,

Pour éviter la saturation du réseau par les messages, l'utilisateur doit limiter la liste des destinataires aux utilisateurs directement concernés par ce message.

Aussi, il doit :

- utiliser avec discernement les listes de diffusion personnelles ou collectives,
- éviter d'envoyer des copies à un nombre injustifié de destinataires,
- s'interdire d''envoyer ou de répondre aux messages en masse ou en chaine,
- ne pas transférer de pièces jointes exécutables, les écrans de veille et les fichiers de type médias (musique, audio, vidéo…).
- vérifier la cohérence entre l'expéditeur présumé et le contenu du message et vérifier son identité. En cas de doute, ne pas hésiter à contacter directement l'émetteur du mail;
- éviter d'ouvrir les pièces jointes provenant d'expéditeurs inconnus dont le titre ou le format paraissent incohérents avec les fichiers envoyés habituellement.

3.8. ACTIVITÉS INTERDITES

Il est interdit de consulter, charger, stocker, publier ou diffuser via les moyens informatiques et de communication, des documents, informations, programmes, images, fichiers, .etc.., contraire à la loi et plus particulièrement les données

- à caractère violent, pornographique contraires aux bonnes mœurs, ou susceptibles de porter atteinte au respect de la personne humaine et de sa dignité ainsi qu'à la protection des mineurs,
- à caractère diffamatoire et de manière générale illicite,
- portant atteinte aux ressources de l'agence,
- portant atteinte à la confidentialité des informations et des données de l'agence et/ou de ses utilisateurs,

- portant atteinte à l'image interne et externe de l'agence de voyage,
- relatifs à la vie privée d'une personne ou à son image, sans autorisation préalable,
- protégés par les lois sur la propriété intellectuelle, autres que ceux qui sont mis à sa disposition et expressément autorisés par la direction.

Ainsi, il est formellement interdit :

- d'utiliser des programmes qui saturent les ressources ou inondent la bande passante,
- d'introduire des programmes nuisibles (cheval de Troie, virus, ou autres),
- d'effectuer des actes de piratage ou d'espionnage,

- Fin du document --