

# **Diagnostic et préconisations quant à l'usage de l'informatique pour la Ligue Centre-Val de Loire Tennis de Table**

Par Quentin BROSSARD,  
Étudiant en 2ème année de BTS SIO - SISR

# Sommaire

- I) Inventaire informatique de l'organisation (3)
- II) Bonnes pratiques informatiques (4)
- III) Connaître le système d'information (15)
- IV) Authentifier et contrôler les accès (16)
- V) Sécuriser les postes (18)
- VI) Tableau récapitulatif (20)

# I) Inventaire informatique de l'organisation

## - 4 PCs fixes (Windows):

- PC-Isabelle : 192.168.1.106 (Câblé)
- PC-Bruno-SIMON : 192.168.1.15 (Wireless)
- PC-Blanc-Lenovo : 192.168.1.43 (Wireless)
- Ancien-PC-Isabelle : 192.168.1.69 (Câblé)

## - 2 PCs portables :

- MacBook-Pro-de-Romain (Mac) :  
192.168.1.14 (Wireless)
- PC-Portable-Isabelle (Windows):  
192.168.1.46 (Wireless)

### LiveBox

IP : 192.168.1.1

Opérateur : Orange

Modèle : 4

### Switch :

Marque : TP-LINK

Modèle : TL-SF1008D

## - 1 Serveur :

- Serveur Windows 2008 x64 : 192.168.1.254

## - 1 Imprimante :

- IP : 192.168.1.200
- Marque : Konica Minolta
- Modèle : bizhub C258

## - 2 Téléphones (1 seul utilisé) :

- IP : 192.168.1.45
- Marque : Cisco
- Modèle : 7800 Series

## II) Bonnes pratiques informatiques

- 1 / Choisir avec soin ses mots de passe (5)
- 2 / Mettre à jour régulièrement vos logiciels (6)
- 3 / Quelle session utilisée ? (7)
- 4 / Effectuer des sauvegardes régulières (8)
- 5 / Faire attention avec son accès Wi-Fi (9)
- 6 / Protéger ses données lors de ses déplacements (10)
- 7 / Être prudent lors de l'utilisation de sa messagerie (11)
- 8 / Télécharger ses programmes sur les sites officiels des éditeurs (12)
- 9 / Être vigilant lors d'un paiement sur Internet (13)
- 10 / Séparer les usages personnels des usages professionnels (14)

# II) Bonnes pratiques informatiques

## 1 / Choisir avec soin ses mots de passe

Il y a deux méthodes connues aidant à la création de mots de passe à partir d'une phrase facile à retenir pour vous :

- Phonétique :

« J'ai acheté 5 CDs pour cent euros cet après-midi » devient Ght5CD%E7am

- Premières lettres :

« Avec la Ligue du Centre de Tennis de Table Vivez au cœur du Ping ! » devient ALLdCdTdTVacdP!

Il est préconisé de ne jamais utiliser le même mot de passe, c'est pourquoi certains utilisent une méthode en plus de la première citée : **\*base du mot de passe\***+**\*fonction où on l'utilise\***

Exemple : Mot de passe pour le site Amazon : Ght5CD%E7amAmazon

Mot de passe pour l'adresse e-mail : Ght5CD%E7ame-mail

## II) Bonnes pratiques informatiques

### 2 / Mettre à jour régulièrement vos logiciels

**Mettre à jour** ses logiciels. Les correctifs et mises à jour servent, entre autre, à corriger les failles et vulnérabilités de ceux-ci.

Mettre à jour **son système** (Windows, Linux, Mac, etc.) par soi-même si aucun service informatique n'est présent dans l'entreprise est vital.

Il ne faut pas hésiter à **y passer du temps si nécessaire**.

Configurer le logiciel pour que les mises à jour se fassent automatiquement, souvent proposé à l'installation du logiciel si l'option est disponible.

## II) Bonnes pratiques informatiques

### 3 / Quelle session utilisée ?

**Sur chaque ordinateur, on peut choisir sa session au démarrage, il est recommandé de créer au moins deux sessions :**

- **Session Administrateur** : possède tous les droits sur le système de l'ordinateur, utile à l'administration du PC, à l'installation et mise à jour de logiciels, etc.
- **Session Utilisateur** : possède des droits restreints, à utiliser dans l'utilisation quotidienne : naviguer sur Internet, lire ses mails, utilisation de ses logiciels, etc.

### **Pourquoi distinguer ces deux types de session ?**

Si vous ne possédez qu'une seule et unique session, celle-ci possède les droits d'administrateur. Une fausse manipulation sur un site Web, un téléchargement frauduleux à partir de ses mails... Une seule erreur et l'attaquant pourrait utiliser vos droits d'administrateur pour **s'infiltrer dans votre machine et votre réseau**.

## II) Bonnes pratiques informatiques

### 4 / Effectuer des sauvegardes régulières

Une **sauvegarde** quotidienne, hebdomadaire ou mensuelle (au maximum) est **fondamentale**. Une inondation, un incendie, une panne électrique, une attaque, tant de possibilités pouvant **réduire à néant** des centaines de fichiers importants ainsi que des années de travail qui n'étaient stockés que sur une machine ou un serveur.

Une sauvegarde peut être effectuée sur :

- Un disque dur externe (à stocker hors de l'organisation ensuite) ;
- Le Cloud (chiffrer les données à l'aide d'un logiciel spécialisé pour sécuriser les informations avant).



## II) Bonnes pratiques informatiques

### 5 / Faire attention avec son accès Wi-Fi

L'accès au Wi-Fi d'une organisation se doit d'être restreint. Si possible, préférer **une connexion Ethernet (filaire)** qui, en plus de proposer une meilleure connexion, permet d'**être sûr** que personne d'extérieur à l'organisation (depuis la rue, le trottoir) ne peut utiliser le réseau sans rentrer dans le(s) bâtiment(s).

**Si impossible, alors il faut sécuriser son accès Wi-Fi :**

- Modifier le mot de passe d'administration de la Box (accès par 192.168.1.1 sur Internet dans notre cas) ;
- Modifier la clé de connexion du Wi-Fi donnée par défaut (au dos de la Box) ;
- Activer la fonction pare-feu disponible sur la Box ;
- Désactiver la Box si non utilisée. Planifier des horaires d'activation du Wi-Fi, attention à ne pas lancer de téléchargements nocturnes si vous n'avez pas modifié la plage horaire en conséquence ;
- Ne jamais utiliser les Wi-Fi publics qui sont bien trop vulnérables.

## II) Bonnes pratiques informatiques

### 6 / Protéger ses données lors de ses déplacements

A l'extérieur, il faut faire attention à son matériel contenant des données liées à l'organisation. Ne pas hésiter à copier les données inutiles à votre mission à l'extérieur sur un disque dur externe et les supprimer de votre support le temps de cette mission.

**Ne laissez personne utiliser votre matériel, même pour une simple recherche, ni utiliser son matériel sur vos supports.**

Exemple : Laisser quelqu'un recharger son téléphone sur votre ordinateur portable peut octroyer des droits sur les fichiers de votre équipement.

## II) Bonnes pratiques informatiques

### 7 / Être prudent lors de l'utilisation de sa messagerie

Les mails et pièces jointes associées jouent un **rôle important** dans un grand nombre d'attaques informatiques.

Il faut :

- Ne pas ouvrir de **pièces jointes** provenant d'inconnus ;
- Ne pas se fier à l'**adresse e-mail du destinataire**, elle peut être falsifiée, il est possible d'envoyer un mail au nom d'une adresse e-mail sans y avoir accès ;
- Faire attention à l'**extension d'un fichier** (.exe, .docx, etc.) si celle-ci vous est inconnue, posez-vous des questions avant de l'ouvrir, faites des recherches, même si le destinataire vous est connu (cf. point au-dessus) ;
- Vérifier les **liens reçus** dans les mails en passant votre pointeur de souris dessus, même si le destinataire vous est connu (cf. point Ne pas se fier à l'adresse e-mail du destinataire) ;
- Ne pas répondre aux mails demandant des informations personnelles ou confidentielles.

## II) Bonnes pratiques informatiques

### 8 / Télécharger ses programmes sur les sites officiels des éditeurs

**Afin de veiller à la sécurité de votre machine et de vos données lors d'un téléchargement :**

- Télécharger vos programmes sur les **sites de leurs éditeurs** ou d'autres **sites de confiance** ;
- **Décocher toutes les cases** proposant d'installer des logiciels complémentaires ;
- **Ne pas croire les publicités** sur un site, même si vous pensez qu'elle amène à un site ou lance un téléchargement, faites la recherche par vous-même si vous souhaitez alors sur le site ou obtenir le téléchargement en question.

## II) Bonnes pratiques informatiques

### 9 / Être vigilant lors d'un paiement sur Internet

Même si un site d'achat en ligne peut paraître professionnel, il peut être **vulnérable** et une fois vos coordonnées bancaires entrées, il sera trop tard.

C'est pour cela que des vérifications s'imposent :

- Vérifier la présence d'un **cadenas** à gauche du lien dans la barre d'adresse ;
- Vérifier la présence de la mention « **https://** » et non pas seulement « **http://** » dans le lien du site Internet, celui-ci fait gage de sécurité ;
- Vérifier l'exactitude de l'adresse du site Internet, qu'il n'y ait pas de fautes d'orthographe.

Exemple : « ***https://amason.com*** » à la place de « ***https://amazon.com*** »

## II) Bonnes pratiques informatiques

### 10 / Séparer les usages personnels des usages professionnels

Il est recommandé de séparer vos usages personnels de vos usages professionnels, vos équipements sont souvent moins protégés que ceux de votre organisation et si un attaquant arrive à prendre le contrôle de vos appareils, il aura en plus accès à vos données professionnelles.

C'est pourquoi, si possible :

- Ne faites pas parvenir vos mails professionnels sur vos e-mails personnels ;
- Ne stockez pas d'informations professionnelles sur vos clés USB, téléphones personnels...

## III) Connaître le système d'information

### 1 / Maintenir un schéma du réseau à jour

Voir fichier Infra\_Ligue.pdf

Créé sur Cisco Packet Tracer (fichier : Infra\_Ligue.pkt).  
Dernière version datant du 14/10/2020.

### 2 / Autoriser à utiliser le Wi-Fi **seulement les appareils autorisés**

Moins il y a d'appareils connectés sur le Wi-Fi, moins le risque de problèmes est élevé et plus la connexion est fluide.

## IV) Authentifier et contrôler les accès

### 1 / Définir des règles de **choix** et de **dimensionnement** des mots de passe

Un mot de passe peut être tordu, s'il est trop court, il est très peu protecteur. Un mot de passe se doit d'avoir une longueur acceptable (souvent 8 à 10 caractères minimum demandé).

Exemple : Calculons le nombre de possibilités de mots de passe à 4 caractères puis à 8 caractères ne comportant que les chiffres de 0 à 9 et l'alphabet en minuscule et majuscule soit 62 caractères différents.

$62^4 = 14\,776\,336$  possibilités

$62^8 = 218\,340\,105\,584\,896$  possibilités

On peut facilement comprendre que la longueur d'un mot de passe impacte grandement sur sa protection.



## IV) Authentifier et contrôler les accès

### 2 / **Modifier** les éléments d'authentification par défaut sur les équipements et services

Certains équipements et services possèdent un mot de passe **par défaut**, un attaquant essayera toujours ce mot de passe puis tous les classiques comme « 0000 », « azerty », etc. C'est pourquoi il faut **absolument** changer le mot de passe qu'on vous donne au départ.

## V) Sécuriser les postes

### 1 / Mettre en place un niveau de sécurité minimal sur tout l'équipement de la structure

Pour cela, **il faut** :

- **Limiter** les applications installées, **supprimer** les logiciels inutiles et **mettre à jour** ceux que vous gardez ;
- Être sûr que vos équipements possèdent un **antivirus** et un **pare-feu** local **actif** et **à jour**. Attention à ne pas posséder deux logiciels de protection différents, ceux-ci risqueraient de se gêner entre eux. Si possible, posséder un parc antivirus homogène ;
- **Désactiver** les exécutions automatiques (autorun) : Panneau de configuration → Matériel et Audio → Exécution automatique → Décocher « Utiliser l'exécution automatique pour tous les médias et tous les périphériques ».

## V) Sécuriser les postes

### 2 / Se protéger des menaces relatives à l'utilisation de supports amovibles

Supports amovibles : Clés USB, disques durs externes, etc.

Ne **jamais** utiliser de supports amovibles :

- Trouvés ;
- Donnés par un inconnu.

Il est possible que ces supports amovibles possèdent un logiciel ou programme développé par un attaquant, si vous le branchez sur un appareil, celui-ci et son réseau pourraient être infectés.

## VI) Tableau récapitulatif

Action	Effectuée	Préconisée si non effectuée	Commentaires
Posséder un inventaire informatique à jour	X		À garder à jour
Posséder différents mots de passe forts (longueur et difficulté à définir)	X	X	À effectuer partout ou au moins sur les endroits sensibles
Mettre à jour ses logiciels	X	X	À faire en continu
Posséder deux sessions « Administrateur » et « Utilisateur » sur chaque PC		X	Permet d'améliorer la sécurité
Effectuer des sauvegardes des données importantes	X		Disque dur externe laissé en permanence avec le serveur

## VI) Tableau récapitulatif

Action	Effectuée	Préconisée si non effectuée	Commentaires
Modifier le mot de passe d'administration de la Box		X	Actuellement par défaut
Modifier la clé de connexion du Wi-Fi		X	Actuellement par défaut
Activer la fonction pare-feu sur la Box	X		Actuellement sur Faible, améliorable ?
Planifier des horaires d'activation du Wi-Fi		X	Si ça ne dérange pas le travail
Posséder un schéma du réseau à jour	X		À garder à jour

## VI) Tableau récapitulatif

Action	Effectuée	Préconisée si non effectuée	Commentaires
Supprimer les logiciels inutiles	X		À continuer sur tous les PCs : utiliser Revo Uninstaller
Posséder un antivirus et un pare-feu local sur chaque équipement	X		Supprimer McAfee via Revo Uninstaller si non déjà fait
Désactiver les exécutions automatiques (autorun)	X	X	À effectuer sur MacBook Romain
Posséder un parc antivirus homogène		X	Actuellement plusieurs antivirus différents utilisés