# INFORMATIQUE
# SECURITE DU MATERIEL
# ET DES LOGICIELS

Incendie, dégât des eaux, vol, piratage, virus, malveillance,... les systèmes informatiques doivent être protégés.

Bien sûr, heureusement, les cabinets dentaires ne sont pas pour l'instant les plus exposés, encore qu'il soit nécessaire d'être méfiant avec le développement des accès aux réseaux distants (Internet, télétransmission,…).

C'est peut-être là, que se situe l'intérêt d'utiliser les services d'un fournisseur d'accès sécurisé.

Pour autant, un certain nombre de précautions doivent être prises.

Si les grandes entreprises, utilisant de gros systèmes, ont depuis longtemps appréhendé ce problème, il ne semble pas que ce soit le cas des plus petites pour lesquelles un certain laxisme est de mise.

Nous l'avons vu dans le chapitre concernant l'ergonomie, le système informatique devra être placé à un endroit où il sera commode à utiliser.

Mais il faudra veiller aussi à ce qu'il soit, autant que faire se peut, à l'abri de l'eau (conduite passant à proximité, projections,...), des poussières (de résine, de plâtre,...), des vibrations (compresseur,...).

**• L'alimentation électrique et ses caprices :**

Micro coupures, surtensions, baisses de tension brutale, coupures momentanées de l'alimentation secteur, ne sont pas appréciées par le matériel informatique.

En général, au cabinet, ces événements ne sont pas désastreux dans la mesure où, en principe, on ne perd que l'information que l'on était en train de traiter. Mais cela est tout de même franchement désagréable, surtout si le phénomène est répétitif.

Nous savons que E.D.F. se doit de nous fournir un courant électrique de 220 V de tension avec une tolérance de ± 10 %.

En cas de problèmes répétés, il est toujours possible de demander à ce service public de procéder au contrôle de la qualité du courant électrique reçu.

Sous réserve, bien entendu, que l'installation électrique interne du local professionnel soit correcte.

A ce propos, il existe des systèmes de prises de courant dits "spécial informatique" comportant des protections diverses (y compris anti-foudre) qui apporteront une certaine sécurité à votre matériel. (interrogez votre électricien favori)

En dernier ressort, il restera toujours la solution de l'onduleur, qui est un dispositif (placé entre la prise de courant et l'ordinateur) qui maintient à un niveau constant l'alimentation électrique et prend instantanément le relais en cas de coupure. Si pendant longtemps le coût de ce type d'appareil était prohibitif, la baisse des tarifs le rend désormais abordable. Dans les configurations en réseau, comportant un serveur de fichiers, il peut être recommandé pour celui-ci.

**• LA SAUVEGARDE, CLEF DE LA SECURITE :**

Quels que soient les systèmes utilisés, personne ne peut se prétendre à l'abri d'une défaillance matérielle ou humaine.

Que ce soit à la suite d'un problème matériel ou d'une mauvaise manœuvre, la restauration de l'environnement de travail ne pourra se faire qu'à partir d'une copie de secours.

**La réalisation de cette copie s'appelle une sauvegarde. Elle est indispensable et doit être systématique.**

Tous les logiciels dentaires comportent une procédure pour la réaliser.

Les supports utilisés varient avec la quantité de données à sauvegarder, généralement un jeu de disquettes suffira ou si nécessaire des cartouches du type Zip™.

**Ces sauvegardes ou copies de secours seront placées en lieu sûr.**

Dans notre cas, une politique de sauvegarde efficace prévoira des rotations quotidiennes à l'aide de supports distincts afin de limiter les risques de pertes de données entre deux sauvegardes.

Ainsi, nous aurons un support de sauvegarde par jour de travail (lundi, mardi, mercredi,...), de cette façon, en cas de malheur, nous ne perdrons, au pire, que les données d'une journée (ce qui sera relativement facile à reconstituer).

**• Le vol de matériel, les assurances :**

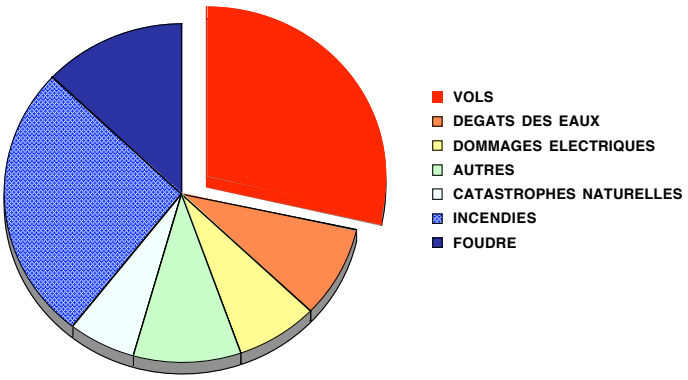
Chaque année, prés de 40 millions de francs en moyenne, représente le coût du sinistre informatique, dans les entreprises Françaises.

Ceci est lié au développement de la micro-informatique et à son utilisation dans les bureaux.

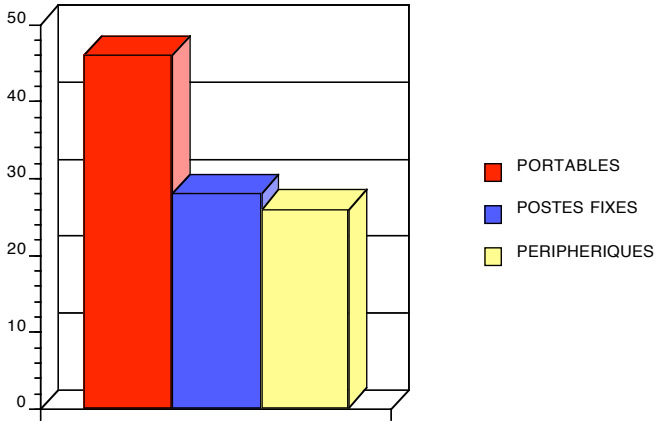
Le vol arrive en tête, suivi par l'incendie, la foudre, le dégât des eaux et les dommages électriques.

En ce qui concerne le vol, les ordinateurs portables, sont les plus convoités. Les principales victimes sont les entreprises de service.

**FREQUENCE DES SINISTRES INFORMATIQUES SUPERIEURS A 100 KF**




**NATURE DES MACHINES VOLEES**




Il sera donc nécessaire de procéder à l'assurance de son matériel informatique que ce soit par le biais de contrats spécifiques ou par extension des contrats déjà existants.

**• Les virus informatiques :**

Régulièrement, la presse, le Net, se font écho d'attaques virales diverses atteignant les parcs micro-informatiques. Ces virus, aux noms aussi exotiques qu'évocateurs, n'ont pas provoqué jusque-là de dégâts à la hauteur des catastrophes annoncées.

Pour autant, la prudence est de mise car les virus existent bien, provoquant ici et là désordres et pertes de données.

Un virus informatique ne s'attaque pas aux circuits intégrés de nos machines mais à la partie logicielle.

D'ailleurs, il est lui-même un programme, conçu pour assurer sa multiplication automatique et qui utilise l'ensemble des média et capacités de stockages comme vecteurs de transmission.

Beaucoup de virus sont prévus pour que leur action soit différée ou ponctuelle, une fois installés dans le système, ils attendront donc le jour et l'heure prévus pour déclencher leur action.

On dénombre environ, 2600 virus dans le monde informatique, tous ne sont pas destructeurs, et certains sont même humoristiques.

Quoi qu'il en soit, la menace ne doit pas être prise à la légère, la grande majorité des attaques virales peut être évitée en prenant quelques précautions simples :

- Contrôler l'accès au système informatique
- Surveiller l'origine des disques utilisées
- Se méfier de la voie télématique (Internet, …)
- Utiliser des logiciels antivirus mis à jour
- Faire systématiquement les sauvegardes

Au cabinet, en principe, le problème ne se pose pas trop, pour l'instant, dans la mesure ou l'ordinateur ne travaille qu'avec des données internes. Qu'en sera-t-il avec la brutale augmentation prévue des connections entre nos ordinateurs et les réseaux externes : Internet, le RSS (Réseau Social de Santé) ?

Il existe pour l'instant deux voies pour accéder au réseau santé social :

- Le concessionnaire officiel : Cégétel qui promet par contrat la sécurité des données et l'absence de virus.
- D'autres fournisseurs d'accès qui se sont insérés entre l'utilisateur et le RSS tels que Wanadoo™ de France Télécom, Liberalis,… qui ne prétendent pas offrir les mêmes garanties pour l'instant.

On sera tout de même bien inspiré de passer au crible (antivirus) avant de les installer sur l'ordinateur, les disques d'origines douteuses, les programmes freeware ou de démonstration, les téléchargements.

Dans ce chapitre et le précédent, nous aurons donc décrit quelques contraintes et désagréments liés à l'informatisation du cabinet dentaire.

Contraintes, dues au respect de la loi (ce qui est la moindre des choses) et qui se traduisent par la petite corvée qui consiste à remplir et expédier la déclaration à la C.N.I.L.

Contraintes issues de l'obligation de télétransmission.

Respect des auteurs en résistant à l'éventuelle envie de réaliser des copies illicites de logiciels, en se souvenant qu'un programme représente toujours un investissement colossal en temps et savoir faire. Récemment d'ailleurs, des entreprises Françaises entre autres en ont fait les frais.

Désagréments, dus aux sinistres divers qui peuvent survenir, comme d'ailleurs, au reste de l'équipement du cabinet et qui nous imposent quelques précautions (assurance, sauvegarde,...).

Virus informatiques dont nous devons connaître l'existence, et contre lesquels, sans céder aucunement à la panique, nous devons savoir nous prémunir.

Mais tous ceci n'est que peu de choses, en comparaison des services que l'informatique nous rend déjà, lesquels logiquement ne devraient que croître et embellir.