Mai 2018

Memo 4 : Cybercriminalité

Vous détenez un ordinateur, un smartphone, une tablette...

URPS CHIRURGIENS DENTISTES AUVERGNE RHÔNE-ALPES

VOUS ÊTES UNE VICTIME POTENTIELLE !

On agit rarement à titre préventif et trop souvent en curatif !
Arrêtons de penser « je ne suis pas concerné(e), ça n'arrive qu'aux autres » !

1. Moyens pour sécuriser vos données

- **Faites des sauvegardes quotidiennement sur un disque dur externe** (stocké dans un lieu sécurisé et *surtout ne le connecter qu'au moment de réaliser la sauvegarde*
- **Utilisez 2 disques durs** (jours pairs / jours impairs)
- **Si vous stockez vos données sur le cloud** : chiffrez les.
- Effectuez **régulièrement des essais de restauration** afin de vérifier la viabilité des sauvegardes
- **Le mot de passe idéal** : 11 à 17 caractères avec lettre minuscule et majuscule + chiffre + signe. Il ne doit pas avoir de lien avec votre vie personnelle ou professionnelle. Ne pas le communiquer. Le changer tous les 6 mois. Eviter de l'enregistrer sur un logiciel de gestion de mots de passe et ne pas le garder sur papier à proximité de la machine.
- **Cryptez vos données sensibles**. Vous trouverez des logiciels de cryptage sur le site de l'ANSSI.
- **Méfiez-vous du wi-fi gratuit** peu sécurisé qui rend vos données accessibles à tous.
- **Éteignez vos ordinateurs** lorsque vous quittez le cabinet.
- Pensez **à fermer votre session** d'ordinateur à chaque fois que vous quittez votre poste de travail.
- **Retirez puis rangez** dans un lieu sécurisé **votre carte CPS**, tous les jours. Ne pas laisser le code à proximité.
- **Utilisez un antivirus** sur votre ordinateur, tablette, smartphone **:** mises à jour régulières
- **Utilisez un antispam** (*ex : mail in black ou Altospam*)
- **Utilisez un destructeur de documents** à coupe croisée.
- **Rédigez et faire signer à tout le personnel du cabinet (*chaque année*) un document avec les informations suivantes :**
  - *Interdiction d'aller sur des sites non professionnels*
  - *Ne pas communiquer le code wifi du cabinet*
  - *Attention à l'ouverture des pièces jointes des mails professionnels*
  - *Aucune personne étrangère au cabinet (même un patient) n'utilise les ordinateurs du cabinet*
  - *Pas de prise en main à distance sans l'autorisation du titulaire ou du responsable informatique*
  - *Aucune clef USB extérieure n'est utilisée sur les ordinateurs du cabinet*

2. Le RANSOMMWARE = Cyber échange : "vos données contre de l'argent"

Fonctionnement : vous recevez un mail avec un lien / PJ. Dès l'ouverture, vos données sont cryptées. Il vous est alors proposé d'obtenir une clé de déchiffrement moyennant une rançon payable en bitcoins.
Conseil : Ne pas payer. Vous n'êtes pas assurés d'obtenir la clé de déchiffrement vous permettant de récupérer vos données. **Seule méthode sûre à 100 % pour se prémunir de ce type d'agissement : avoir des sauvegardes à jour. Et surtout réfléchir avant de cliquer…**

3. Fiches d'alertes gendarmerie : à télécharger (site de l'Espace Numérique Entreprise)

http://www.ene.fr/informer/ressources-documentaires1/fiches-alertes-gendarmerie.html

URPS CD Auvergne – Rhône Alpes
Siège : 21, quai Antoine Riboud - 69002 Lyon – Confluence / **Contact :** florence.therond@urps-cd-ara.fr

Memo 4 : Cybercriminalité

URPS CHIRURGIENS DENTISTES AUVERGNE RHÔNE-ALPES

4. Soyez vigilant !

- **Au personnel** qui quitte votre cabinet en emmenant des données sensibles.
- Vous êtes une cible dès que vous vous connectez à internet.
- Ne cliquez par sur une pièce jointe ou un lien sans être certain de la provenance.
- **Escroquerie aux faux RIB** : elle touche particulièrement les professionnels de santé. Mettez en place des procédures. Pour cela vous pouvez vous rapprocher de votre établissement bancaire, lequel pourra vous apporter de précieux conseils.
- **CNIL** : En cas de cyberattaque et de mise en ligne de données sensibles, vous risquez d'une part d'être épinglé par la CNIL mais aussi de de perdre la confiance de votre patientèle.
- **Attention :** apprenez à reconnaître les **adresses frauduleuses :**

  > Sur les sites sécurisés vous devez avoir:

  - Adresse web : http – le « s » manque.

  - Absence du cadenas devant le « https » de l'adresse du site.

  > **Dans les mails :**

  - Dans l'adresse de l'expéditeur, bien regarder ce qui figure après le « **@** » (exemple le « ***.fr*** » final remplacé par un « ***.rf*** »).

  En cas de doute, imprimer le mail ; il peut en ressortir des éléments non visibles à l'écran (apparition d'une seconde adresse mail par exemple).
- **Vigilance quant aux e-mails rédigés en mauvais français**

5. Conseils après une cyberattaque

Déconnecter la machine du réseau : permet de stopper l'attaque si elle est toujours en cours. S'il était toujours connecté à la machine, l'intrus n'a plus de contrôle sur celle-ci et ne pourra donc pas surveiller ce que vous faites et/ou modifier des fichiers. En revanche, maintenez la machine sous tension et ne la redémarrez pas, car il serait alors impossible de connaître les processus qui étaient actifs au moment de l'intrusion. Vous risqueriez de provoquer une modification sur le système de fichiers et de perdre de l'information utile pour l'analyse de l'attaque.

Contacter un spécialiste : connu ou identifié près de chez vous sur la plate-forme cybermalveillance.gouv.fr, l'aide aux victimes d'actes de cybermalveillance, qui a déjà recensé, validé et référencé au niveau national quelque 1 300 prestataires à même de vous aider d'un point de vue technique.

Déposer plainte : les agents de police judiciaire ont l'obligation de prendre les plaintes, même sans préjudice. Ces dépôts de plainte permettent d'avoir une meilleure visibilité sur la menace cyber et contribuent à la mise en place de moyens permettant d'y faire face, tant techniques que humains...

Communiquer en interne : Il est impératif que le personnel comprenne l'incident auquel la structure a été confrontée. Le site cybermalveillance.gouv.fr propose des « fiches réflexe » pour informer et communiquer sur chaque type de risque : virus, spam, DDoS (déni de service distribué), etc.

Diffuser au maximum les bonnes pratiques... : prudence lors de l'ouverture des fichiers, mise à jour régulière des systèmes, sauvegardes. De façon générale, ne pas considérer que les investissements en sécurité informatique sont inutiles : il est important de faire appel à des prestataires dont c'est le métier !

« La confiance n'exclut pas le contrôle »

ce principe doit s'appliquer à tous ceux qui vous entourent.

URPS CD Auvergne – Rhône Alpes

URPS CD ARA : 15 rue du Pré la Reine – 63000 Clermont Fd / **Contact :** florence.therond@urps-cd-ara.fr – 06.47.43.70.21