la médicale
assure les professionnels de santé

Guide de prévention

pour la protection de votre système d'information

EN FAIRE +
POUR VOTRE ACTIVITÉ

Les 12 bonnes pratiques en informatique

1 CHOISISSEZ AVEC SOIN VOTRE MOT DE PASSE

- Choisissez si possible un mot de passe de 12 caractères différents (majuscule, minuscule, chiffres et caractères spéciaux).
- Utilisez la méthode phonétique : j'ai acheté 5 CD pour 100 € cet après-midi = ght5CD%E7am.

2 METTEZ VOS LOGICIELS À JOUR RÉGULIÈREMENT

- Configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement.
- Utilisez exclusivement les sites internet officiels des éditeurs.

3 SOYEZ ATTENTIFS A VOS UTILISATEURS ET AU CHOIX DE VOS PRESTATAIRES

- Prenez un compte utilisateur pour l'utilisation quotidienne de votre ordinateur : navigation sur internet, consultation des e-mails, utilisation des logiciels de bureautique.
- Utilisez le compte administrateur uniquement pour intervenir sur le fonctionnement global de l'ordinateur : installation ou mise à jour des logiciels, gestion des comptes utilisateurs.

4 EFFECTUEZ DES SAUVEGARDES RÉGULIÈRES

- Utilisez des supports externes tels qu'un disque dur externe réservé exclusivement à cet usage.
- Avant de copier vos données sur le « cloud [1] », rendez impossible leur lecture en les chiffrant à l'aide d'un logiciel de chiffrement[2].

5 SÉCURISEZ L'ACCÈS WI-FI DE VOTRE ENTREPRISE

- Lors de votre 1ère connexion, modifiez l'identifiant de connexion et le mot de passe qui vous ont été donnés par votre fournisseur d'accès.
- Modifiez la clé de connexion par défaut par une clé (mot de passe) de plus de 12 caractères différents.
- Activez la fonction pare-feu de votre box.

6 SOYEZ AUSSI PRUDENT AVEC VOTRE SMARTPHONE OU VOTRE TABLETTE QU'AVEC VOTRE ORDINATEUR

- En plus du code PIN, utilisez un mot de passe pour bloquer l'accès à votre terminal et configurez-le pour qu'il se verrouille automatiquement.
- Effectuez régulièrement des sauvegardes sur un support externe.

7 PROTÉGEZ VOS DONNÉES LORS DE VOS DÉPLACEMENTS

- Emportez un filtre de protection écran pour votre ordinateur.
- Désactivez les fonctions Wi-Fi et Bluetooth de vos appareils.
- N'utilisez pas les clés USB qui vous ont été offertes.

[1] Le cloud correspond entre autre à un service en ligne de stockage sécurisé de documents.

[2] Un procédé de cryptographie grâce auquel on rend la compréhension d'un document impossible aux personnes qui ne possèdent pas la clé de déchiffrement.

8 SOYEZ PRUDENT LORS DE L'UTILISATION DE VOTRE MESSAGERIE

- N'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le format paraît incohérent avec les fichiers que l'on vous envoie habituellement.
- Ne répondez pas à un e-mail de demande d'informations personnelles ou confidentielles (code de carte bancaire, code confidentiel).

9 TÉLÉCHARGEZ VOS PROGRAMMES SUR LES SITES OFFICIELS DES ÉDITEURS

- Décochez ou désactivez les cases proposant d'installer des logiciels complémentaires.
- Désactivez l'ouverture automatique des documents téléchargés et lancez une analyse anti-virus avant de les ouvrir.

10 SOYEZ VIGILANT LORS D'UN PAIEMENT SUR INTERNET

- Assurez-vous que la mention « https:// » apparaît au début de l'adresse du site internet.
- Vérifiez l'exactitude de l'adresse du site internet en prenant garde aux fautes d'orthographe.

11 SÉPAREZ VOS USAGES PERSONNELS DES USAGES PROFESSIONNELS

- N'hébergez pas de données professionnelles sur vos équipements personnels (clé USB).
- Ne connectez pas de supports amovibles personnels (clés USB, disques durs externes) aux ordinateurs de l'entreprise.

12 PRENEZ SOIN DE VOS INFORMATIONS PERSONNELLES, PROFESSIONNELLES ET DE VOTRE IDENTITÉ NUMÉRIQUE

- Décochez les cases qui autorisent les sites à conserver vos données personnelles.
- Donnez accès au minimum d'informations personnelles et professionnelles sur les réseaux sociaux.

Aller + loin

Afin de renforcer efficacement la sécurité de vos équipements communicants et de vos données, vous pouvez compléter les 12 bonnes pratiques de ce guide par les mesures suivantes :

- Désignez un correspondant/référent pour la sécurité informatique.
- Chiffrez vos données et vos échanges d'information à l'aide de logiciels de chiffrement.
- Durcissez la configuration de votre poste et utilisez des solutions de sécurité éprouvées (pare-feux, antivirus).
- Avant d'enregistrer des fichiers provenant de supports USB sur votre ordinateur, faites-les analyser par un antivirus.
- Désactivez l'exécution automatique des supports amovibles depuis votre ordinateur.
- Éteignez votre ordinateur pendant les périodes d'inactivité prolongée (nuit, week-end, vacances...).
- Surveillez votre système, notamment en utilisant les journaux d'événements, pour réagir aux événements suspects (connexion d'un utilisateur hors de ses horaires habituels, transfert massif de données vers l'extérieur de l'entreprise, tentatives de connexion sur un compte non actif...).

Pour plus d'information, vous pouvez télécharger le dossier complet « Guide des bonnes pratiques de l'informatique* » disponible sur notre site internet : **www.lamedicale.fr**

* Source : « Guide des bonnes pratiques de l 'informatique »
Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), mars 2015

En cas d'incident informatique

EN CAS DE FONCTIONNEMENT INHABITUEL DE VOTRE ORDINATEUR :

Connexion impossible, activités inhabituelles, services ouverts non autorisés, fichiers créés, modifiés ou supprimés sans autorisation...

CE QUE VOUS DEVEZ FAIRE :

1. Déconnectez votre matériel du réseau. En revanche, maintenez-le sous tension et ne le redémarrez pas, pour ne pas perdre d'informations utiles.
2. Faites appel à votre prestataire informatique habituel dans un délai raisonnable après constatation de l'incident.
3. Si votre prestataire informatique ne peut pas résoudre le problème affectant votre système car il suppose une cyber-attaque, vous devez compléter avec lui **la Déclaration de cyber-sinistre** et l'envoyer à notre prestataire d'assistance cyber par email : **lamedicale.cyberassistance@thalesgroup.com** ou par fax au **01 73 32 22 77.**
4. Votre prestataire informatique devra suivre l'ensemble des recommandations de notre prestataire d'assistance cyber jusqu'au confinement de l'incident.

ⓘ Dans le cas où vous ne disposez pas de prestataire informatique, notre prestataire d'assistance cyber vous fournira une liste de prestataires informatiques. Notre prestataire d'assistance cyber ne pourra intervenir si et seulement si vous avez contractualisé avec un prestataire informatique au préalable.

EN CAS DE PERTE D'EXPLOITATION SUITE À UNE CYBER-ATTAQUE :

Veuillez compléter et renvoyer votre Déclaration de sinistre Multirisque Professionnelle à l'adresse suivante :

LA MÉDICALE DE FRANCE - Service Sinistres Multirisque
3, rue Saint-Vincent-de-Paul - 75499 Paris Cedex 10

EN CAS DE MISE EN CAUSE DE VOTRE RESPONSABILITÉ CIVILE PROFESSIONNELLE SUITE À UNE CYBER-ATTAQUE :

Veuillez envoyer votre déclaration écrite à l'adresse suivante :

LA MÉDICALE DE FRANCE - Service Sinistres Multirisque
3, rue Saint-Vincent-de-Paul - 75499 Paris Cedex 10

La Médicale de France, entreprise régie par le Code des assurances. Société anonyme d'assurances au capital de 2 160 000 € entièrement versé.
582 068 698 RCS PARIS. Siège social : 50-56, rue de la Procession 75015 PARIS. **Adresse de correspondance :** 3, rue Saint-Vincent-de-Paul 75499 PARIS Cedex 10.
Document à caractère publicitaire.

12BP 4771 – 04/2017