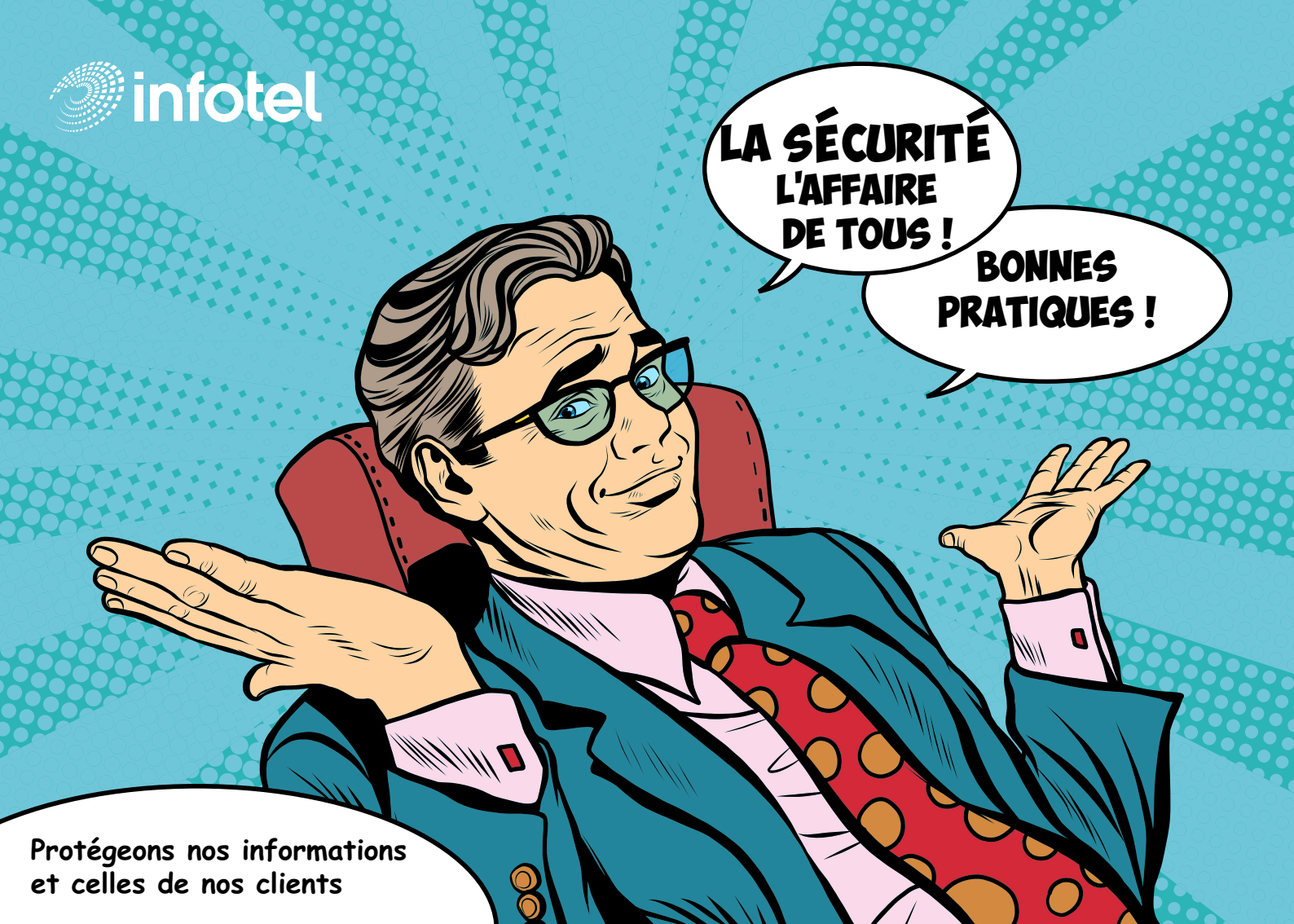
infotel
LA SÉCURITÉ L'AFFAIRE DE TOUS !
BONNES PRATIQUES !
Protégeons nos informations et celles de nos clients

✔ **METTRE EN PLACE** une politique de sécurité de notre système d'informations.

✔ **GARANTIR** la disponibilité, la confidentialité, l'intégrité de l'information et des moyens de preuve et de contrôle.

✔ **RÉPONDRE** aux attentes de nos clients qui, dans le cadre de leurs projets, émettent des exigences en matière de sécurité de l'information.

Protégeons nos informations et celles de nos clients

1 GÉRER SON MOT DE PASSE

Le mot de passe est un élément de sécurité strictement personnel et confidentiel et ne doit pas être communiqué à autrui.

Le système, mis en place par Sesame, vous demande de changer votre mot de passe tous les 60 jours.
Le mot de passe ne peut être identique aux 10 mots de passe précédents.

IL DOIT :

- → Comporter au moins 8 caractères (l'idéal étant 12 caractères) ;
- → Contenir des minuscules, des majuscules, des chiffres et des caractères spéciaux et accentués.

IL NE DOIT PAS CONTENIR :

- → Une chaîne de caractères extraite de votre nom, adresse électronique, etc. ;
- → Un mot figurant dans un dictionnaire quel qu'il soit (même écrit à l'envers) ;
- → Une date ;
- → Un code ou numéro tel que numéro de Sécurité Sociale, plaque d'immatriculation de véhicule, etc. ;
- → Un caractère répété (exemple : 55555).

Protégeons nos informations et celles de nos clients

2 LE BON USAGE D'INTERNET AU TRAVAIL

L'usage d'internet dans le cadre de vos missions est réservé à un usage professionnel conformément au livret d'accueil et au règlement intérieur.

→ Le collaborateur ne doit pas, sans y avoir été autorisé par Infotel Conseil, adhérer à un forum de discussion, s'abonner à des listes de diffusion, télécharger des logiciels ou données en provenance du réseau internet.

→ L'usage d'internet fait l'objet d'une surveillance permettant à Infotel Conseil de contrôler l'activité et d'identifier les dérives d'utilisation prohibées par la législation ou les règles internes à Infotel Conseil.

3 LE BON USAGE DE VOTRE MESSAGERIE PROFESSIONNELLE

→ Règle n°1 : utiliser l'email à bon escient

- Ne pas oublier le téléphone pour gérer une urgence et pour plus de rapidité ;
- Penser aux réunions (Visioconférence ou présentiel).

→ Règle n°2 : faciliter l'exploitation de vos e-mails

- Destinataire = pour action ;
- Copie = pour information ;
- Mettre un texte explicite dans l'objet ;
- Éviter trop de destinataires.

→ Règle n°3 : veiller au contenu des courriels

- Bien relire votre email ;
- Message court et clair ;
- Éviter l'humour et le second degré ;
- Prêter attention aux informations confidentielles ;
- Proscrire les injures.

→ Règle n°4 : évitez les emails ping-pong

Au bout de deux allers/retours, il est judicieux de passer au téléphone...

→ Règle n°5 : ne pas utiliser l'email pour résoudre un conflit

→ Règle n°6 : organiser sa boîte de messagerie

Protégeons nos informations et celles de nos clients

4 ACCÉDER AUX LOCAUX D'INFOTEL

Restons vigilants

Toute personne étrangère à l'entreprise sans badge doit être dirigée vers l'accueil ou vers un responsable.

Ce qu'il faut retenir :

- Votre badge d'accès est nécessaire pour entrer et sortir de l'agence ;
- **Votre badge d'accès est strictement personnel ;**
- En cas de perte, il faut immédiatement alerter l'équipe Sesame via le helpdesk ;
- En cas de départ de l'entreprise, le badge doit être restitué à votre responsable ;
- En cas de nécessité de service (premier arrivé, dernier parti) le code de l'alarme vous sera confié.
  Ce code est bien entendu secret. Il ne doit en aucun cas et sous aucun prétexte être divulgué ;
- Toutes les personnes qui n'ont pas de badge pour les locaux sont considérées comme visiteurs ;
- Sans badge, les données suivantes (identité, heure d'arrivée, raison de la visite, personne responsable de l'accueil) sont consignées dans le registre à l'accueil de votre agence ;
- Au moment de son départ, le visiteur restitue le badge.

Protégeons nos informations et celles de nos clients

5 VOUS DEVEZ RÉAGIR

Dans tous les cas informez rapidement l'équipe Sésame par téléphone. Déclarez un incident de sécurité via le helpdesk une fois le réseau rétabli.

Helpdesk Sesame : **09 72 65 55 00**
https://support-sesame.infotel.com/

Lorsque que vous êtes témoin d'un incident touchant à la sécurité du SI, vous devez réagir en informant Sesame au plus vite.

Voici par exemple quelques incidents qui doivent vous faire réagir :

- → La porte de l'agence ne ferme plus ;
- → Vous constatez que des données confidentielles de l'entreprise sont en accès public ;
- → Vous êtes le destinataire de spam sur votre messagerie professionnelle ;
- → Votre ordinateur vous signale un problème de mise à jour de l'antivirus ;
- → Vous êtes victime d'un vol de donnée personnelle ; etc.

Il s'agit d'une faille de sécurité de l'information

Dans ce cas, déclarez un incident de sécurité via le helpdesk Sesame.

- → Vous êtes victime d'un ransomware ;
- → Votre ordinateur est infecté par un virus ;
- → Vous êtes victime du vol de votre PC portable ou de votre mobile ;
- → Vous constatez une intrusion informatique ou physique ;
- → Etc.

Il s'agit d'un incident de sécurité de l'information

En cas d'infection, déconnectez immédiatement votre équipement et déclarez un incident de sécurité via le helpdesk Sesame.

Protégeons nos informations et celles de nos clients

6 INSTALLER UN LOGICIEL SUR SON ORDINATEUR

Pour l'installation de logiciels dans le cadre de votre mission, vous avez à votre disposition deux manières de procéder :

- Infotel a mis à disposition un environnement qui permet d'installer des logiciels et outils sans être administrateur de la machine. Les logiciels disponibles ont été sélectionnés et évalués par l'équipe Sesame. L'objectif est de laisser davantage d'autonomie aux utilisateurs tout en contrôlant les logiciels installés sur le parc informatique de chaque direction régionale ;
- Il est également possible via GLPI (https://support-sesame.infotel.com/) de demander l'installation d'un logiciel sur sa machine (choix Créer une demande – Logiciel – Installation).

1 IDENTIFIER LES DONNÉES IMPORTANTES ET LES PROTÉGER

N'oubliez pas de mentionner en bas de vos documents la classification retenue :

- → Usage interne
- → Usage restreint
- → Confidentiel

Voici quelques règles liées à l'identification des données

- → Identifiez et répertoriez les informations nécessitant des mesures de protection ;
- → En bas de page de vos documents, appliquez la classification de protection :

1• En l'absence de mention : le document est Public.

2• Usage interne : informations circulant à l'intérieur d'Infotel.

3• Usage restreint : informations ne devant être communiquées qu'aux personnes directement concernées et identifiées (personnes internes ou externes).

4• Confidentiel : réservé aux informations dont la divulgation pourrait porter atteinte aux intérêts économiques, stratégiques ou à la sécurité.

Protégeons nos informations et celles de nos clients

8 LA SÉCURITÉ DE VOS OUTILS DE TRAVAIL

→ **Règle n°1 : avoir un antivirus à jour**
Les mises à jour de l'antivirus de votre PC sont automatiques.

→ **Règle n°2 : ne jamais ouvrir une pièce jointe dont l'expéditeur est soit inconnu, soit d'une confiance relative**
Vous éviterez d'introduire un virus ou du code malveillant sur le réseau du SI.

→ **Règle n°3 : mettre ses logiciels à jour**
Ne reportez pas les mises à jour logicielles.

→ **Règle n°4 : ne pas télécharger n'importe quoi**
Téléchargez des logiciels fiables à partir du site de l'éditeur et lisez toujours les conditions d'utilisation des licences.

→ **Règle n°5 : rangez et sauvegardez vos documents au bon endroit**
Stockez vos fichiers sur les disques réseaux sécurisés d'Infotel qui vous garantissent intégrité, disponibilité et confidentialité. Le disque C peut accueillir vos documents personnels (CRA, notes de frais), etc.

→ **Règle n°6 : faites un ménage régulier**

- Prenez soin de votre ordinateur en l'entretenant de façon régulière ;
- Nettoyage physique du PC à l'aide d'une bombe aérosol ;
- Défragmentez le disque dur ;
- Videz la corbeille ;
- Videz le cache du navigateur ;
- Supprimez les cookies ;
- Supprimez les fichiers inutiles.

→ **Règle n°7 : PC portables et smartphones : toujours sous contrôle !**

- Utilisez un câble antivol pour votre PC portable ;
- Ne laissez pas votre smartphone sans surveillance ;
- Verrouillez votre bureau.

Protégeons nos informations et celles de nos clients

9 QUELQUES TRUCS À NE SURTOUT PAS FAIRE !

Liste bien entendu non exhaustive !

- Brancher un lecteur externe personnel (clé USB, disque externe, Smartphone) sur votre ordinateur connecté au réseau Infotel ;
- Ne pas verrouiller sa session en quittant son bureau, même pour une absence de courte durée ;
- Ne pas déclarer une faille de sécurité en pensant qu'un autre le fera ;
- Laisser traîner un document sensible sur un bureau ;
- Ouvrir une pièce jointe ou cliquer sur un lien contenu dans un courriel dont l'expéditeur est « douteux » ;
- Laisser sans surveillance, même momentanément, son smartphone ou son PC portable ;
- Ne pas connecter régulièrement son PC portable sur le réseau de l'entreprise ;
- Désactiver le contrôle d'accès des locaux parce que vous avez oublié votre badge ;
- Sur internet : cliquer sur les tous les boutons des sites qui promettent de « raser gratis » ;
- Ne pas classifier ses documents et ne pas respecter les consignes de stockage car c'est contraignant ;
- Tout ranger sur votre disque C, car c'est bien plus rapide que de passer par les réseaux ;
- Donner votre mot de passe à l'équipe Sesame ou à votre responsable parce qu'ils sont forcément plus « sécuresponsables » que les autres ;
- Expliquer avec moult détails votre travail au premier curieux qui se présente car il a l'air sympa ;
- Inonder vos collègues de messages alors qu'un simple coup de fil ou un échange au coin café aurait amplement suffit ;
- Construire son mot de passe à partir du nom de ses enfants, de son chien ou de sa marque de voiture préférée ;
- Laisser rentrer dans les locaux de l'agence le laveur de carreaux sans lui faire signer le registre des visiteurs ;
- Etc.

Protégeons nos informations et celles de nos clients

10 ENTRAINEZ-VOUS

Testez vos connaissances sur les malwares et ransomwares

1. **Un ransomware est :**
   a. une boîte en plastique hermétique, vendue dans les réunions ransomwares ;
   b. un outil de prise de contrôle à distance utilisé par le helpdesk ;
   c. un programme installé généralement à l'insu de l'utilisateur et qui va prendre en otage les données qui lui sont accessibles ;
   d. un moyen facile de gagner de l'argent pour les organisations criminelles.

2. **Face aux ransomwares, mon anti-virus est :**
   a. pas toujours efficace ;
   b. complètement inefficace ;
   c. le nec plus ultra de la protection ;
   d. capable de lire dans la matrice.

3. **Un malware est :**
   a. une catégorie de logiciel exclusivement réservée aux hommes ;
   b. une catégorie de logiciel qui fait généralement mal à la technologie de l'information ;
   c. un terme générique regroupant virus, vers, chevaux de Troie… (malicious software) ;
   d. une chaîne de magasins de bricolage ouverts le dimanche.

4. **Les solutions suivantes aident à limiter la propagation ou l'installation d'un malware :**
   a. le coup de boule ;
   b. le coup de pied latéral (en pleine face) ;
   c. les solutions de sandboxing ;
   d. les antivirus.

5. **Si je ne suis pas administrateur de ma machine :**
   a. je suis un peu moins exposé aux malwares, mais pas non plus invincible ;
   b. j'ai raté ma vie (surtout après 30 ans) ;
   c. je suis invincible ;
   d. je vais me plaindre auprès du helpdesk.

6. **Sur les Mac :**
   a. les malwares n'existent pas ;
   b. il faut un connecteur particulier pour installer un malware ;
   c. les malwares sont moins fréquents, mais existent (question de parts de marché) ;
   d. les malwares sont une révolution.

Protégeons nos informations et celles de nos clients

10 ENTRAINEZ-VOUS

7. **Je limite le risque d'être infecté par un malware en :**
   a. installant toujours mes programmes depuis le site ou média fourni par l'éditeur légitime du programme ;
   b. récupérant tous mes programmes sur securewarez (le torrent des programmes secure) ;
   c. installant uniquement les programmes dont j'ai réellement besoin pour mon travail ;
   d. me renseignant rapidement sur un programme avant de l'installer (revue, éditeur qui a pignon sur rue, site Web…).

8. **J'ai reçu un mail qui semble provenir de ma banque, ce mail m'invite à cliquer sur un lien :**
   a. je regarde dans le rétro, je mets le clignotant, je clique ;
   b. tu ne m'auras pas comme ça sankukai, je copie-colle le lien dans mon navigateur et je fonce ;
   c. je ne clique pas sur le lien, mais je me connecte (en tapant l'adresse moi-même, ou via un signet) sur le site Web de ma banque… ;
   d. j'appelle un ami.

9. **Les malwares sur téléphones portables :**
   a. comme le yeti, Nessi ou les virus sur mac : c'est un mythe ;
   b. c'est une réalité, pour m'en protéger j'applique les mêmes conseils que sur mon PC et j'évite de jailbreaker mon terminal iOS ou de rooter mon terminal Android ;
   c. sont un peu plus fréquents sur Android que sur iOS ;
   d. n'existent pas sur les tablettes.

10. **Si je suspecte que ma machine ait pu être infectée par un malware :**
    a. je me garde bien de le dire… parce que sinon le responsable sécurité me punit ;
    b. je suis de nature généreuse et donc je partage un maximum de fichiers, mails et documents avec mes collègues ;
    c. je cesse d'utiliser ma machine dès que possible, je la débranche du réseau tout en la laissant allumée et j'avertis immédiatement le helpdesk ;
    d. je la reboote un coup…

Réponses
1. *c - d* ; **2.** *a* ; **3.** *b - c* ; **4.** *c - d* ; **5.** *a* ;
6. *b - c* ; **7.** *a - c - d* ; **8.** *c* ; **9.** *b - c* ; **10.** *c*

D'après Paul Such, Global Security Mag n° 37, octobre-novembre- décembre 2016.

Protégeons nos informations et celles de nos clients

infotel

Protégeons nos informations et celles de nos clients

Helpdesk Sesame : **09 72 65 55 00**

support-sesame.infotel.com