Cybercriminalité

Le *Guide des bonnes pratiques de l'informatique* édité notamment par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) présente douze recommandations qui constituent un corpus incontournable.

1 Choisir avec soin ses mots de passe

Les mots de passe doivent être difficiles à retrouver à l'aide d'outils automatisés ou à deviner. Pour cela, ils doivent comporter **douze caractères de type différent** (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec l'utilisateur (nom, date de naissance...) et ne figurant pas dans le dictionnaire.

Au sein de l'entreprise, il convient de :

1. Déterminer des règles de choix et de dimensionnement (longueur) des mots de passe et de... les faire respecter ;
2. Modifier toujours les éléments d'authentification (identifiants, mots de passe) définis par défaut sur les équipements (imprimantes, serveurs...) ;
3. Ne pas conserver les mots de passe dans des fichiers ou sur des post-it ;
4. Sensibiliser les collaborateurs au fait qu'ils ne doivent pas pré-enregistrer leurs mots de passe dans les navigateurs.

2

Mettre à jour régulièrement ses logiciels

Dans chaque système d'exploitation (Android, IOS, Windows...), logiciel ou application, des vulnérabilités existent.
Une fois découvertes, elles sont corrigées par les éditeurs qui proposent des mises a jour de sécurité. Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les hackers exploitent ces vulnérabilités pour mener à bien leurs attaques.

Au sein de l'entreprise, il convient de :

1. Définir et faire appliquer par l'équipe une politique de mises à jour régulières ;
2. Configurer les logiciels de la société ou du cabinet pour que les mises à jour de sécurité s'installent automatiquement et, à défaut, de télécharger les correctifs de sécurité disponibles ;
3. Utiliser exclusivement les sites Internet officiels des éditeurs.

URPS médecins libéraux Auvergne Rhône Alpes

3

Bien connaître ses utilisateurs et ses prestataires

Lors de l'utilisation quotidienne de son ordinateur, on ne se sert que du compte utilisateur. Le compte administrateur, lui, n'est à utiliser que pour intervenir sur le fonctionnement global de l'ordinateur (gérer des comptes utilisateurs, modifier la politique de sécurité...).

Les systèmes d'exploitation récents permettent d'intervenir facilement sur le fonctionnement global d'une machine sans changer de compte. Le mot de passe administrateur est simplement demandé pour effectuer les manipulations désirées. Le compte administrateur permet d'effectuer d'importantes modifications sur votre ordinateur.

Au sein de l'entreprise, il est impératif de :

1. Réserver l'utilisation du compte administrateur au service informatique si celui-ci existe, sinon d'en protéger l'accès en n'ouvrant pour les employés que des comptes utilisateur ;
2. Identifier les différents utilisateurs du système et les droits qui leur sont accordés ;
3. Supprimer les comptes anonymes et génériques (stagiaire, presse...), chaque utilisateur devant être identifié nommément afin de pouvoir relier une action sur le système à un utilisateur ;
4. Encadrer par des procédures les arrivées et les départs de personnels pour s'assurer que les droits octroyés sur les systèmes d'information sont appliqués au plus juste et qu'ils sont révoqués lors du départ de la personne.

URPS médecins libéraux Auvergne Rhône Alpes

4

Effectuer des sauvegardes régulières

Pour sauvegarder ses données, on peut utiliser des supports externes (disque dur externe réservé exclusivement à cet usage…) que l'on range ensuite dans un lieu éloigné de l'ordinateur, de préférence à l'extérieur du siège social pour éviter que la destruction des données d'origine ne s'accompagne de la destruction de la copie de sauvegarde en cas d'incendie ou d'inondation, ou que la copie de sauvegarde ne soit volée en même temps que l'ordinateur.

URPS médecins libéraux Auvergne Rhône Alpes

5

Sécuriser l'accès Wi-Fi de votre entreprise

Un Wi-Fi mal sécurisé peut permettre à des personnes d'intercepter vos données et d'utiliser la connexion Wi-Fi à votre insu pour effectuer des opérations malveillantes.

C'est pourquoi l'accès à Internet par un point d'accès Wi-Fi est à éviter dans le cadre professionnel : une installation filaire est plus sécurisée et plus performante. Si le Wi-Fi est le seul moyen possible d'accéder à Internet, il convient de sécuriser l'ensemble en configurant la borne d'accès à Internet, notamment en modifiant la clé de connexion par défaut par une clé (mot de passe) de plus de douze caractères de types différents.

URPS médecins libéraux Auvergne Rhône Alpes

6

Être aussi prudent avec son ordiphone ou sa tablette qu'avec son ordinateur

Les ordiphones (Smartphones) sont très peu sécurisés.

Il est donc indispensable :

1. De n'installer que les applications nécessaires et vérifier à quelles données elles peuvent avoir accès avant de les télécharger ;
2. En plus du code PIN qui protège la carte téléphonique, utiliser un schéma ou un mot de passe pour sécuriser l'accès au terminal et le configurer pour qu'il se verrouille automatiquement ;
3. Effectuer des sauvegardes régulières des contenus sur un support externe ;
4. Ne pas pré-enregistrer les mots de passe.

7

Protéger ses données lors de ses déplacements

Voyager avec des appareils nomades fait peser des menaces sur des informations sensibles en cas de vol ou de perte.

Il convient donc de n'utiliser que du matériel dédié à la mission et ne contenant que les données nécessaires, ou encore d'éviter de connecter ses équipements à des postes qui ne sont pas de confiance.

Autre précaution : ne jamais utiliser les clés USB offertes lors des déplacements car elles sont susceptibles de contenir des programmes malveillants.

URPS médecins libéraux Auvergne Rhône Alpes

8

Être prudent lors de l'utilisation de sa messagerie

Les courriels et leurs pièces jointes jouent un rôle central dans les attaques informatiques. Des précautions sont donc à prendre :

1. Vérifier la cohérence entre l'expéditeur présumé et le contenu du message et vérifier son identité ;
2. Ne pas ouvrir les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents ;
3. Si des liens figurent dans un courriel, passez votre souris dessus avant de cliquer. L'adresse complète du site s'affichera dans la barre d'état du navigateur, ce qui permet d'en vérifier la cohérence ;
4. Ne jamais répondre par courriel à une demande d'informations personnelles ou confidentielles car il s'agit d'attaques par hameçonnage ;
5. Ne pas ouvrir ni relayer des messages de types alerte virale, etc. ;
6. Désactiver l'ouverture automatique des documents téléchargés et lancer une analyse antivirus avant de les ouvrir.

URPS médecins libéraux Auvergne Rhône Alpes

9

Télécharger ses programmes sur les sites officiels des éditeurs

Télécharger du contenu numérique sur des sites Internet dont l'origine n'est pas assurée, c'est prendre le risque d'enregistrer sur son ordinateur des programmes ne pouvant être mis à jour et qui, le plus souvent, contiennent des virus ou des chevaux de Troie.

Dans ce contexte, il est recommandé de :

1. Télécharger les programmes sur les sites de leurs éditeurs ou d'autres sites de confiance ;
2. Décocher ou désactiver toutes les cases proposant d'installer des logiciels complémentaires ;
3. Réfléchir avant de cliquer sur des liens sponsorisés ; désactiver l'ouverture automatique des documents téléchargés et lancer une analyse antivirus avant de les ouvrir.

10

Être vigilant lors d'un paiement sur Internet

Avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications.

Dans ce contexte, il est recommandé de :

1. Contrôler la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet ;
2. S'assurer que la mention « https:// » apparaît au début de l'adresse du site Internet ;
3. De vérifier l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe ;
4. Privilégier la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS ;
5. Ne jamais transmettre le code confidentiel de sa carte bancaire.

11

Séparer les usages personnels des usages professionnels

Il est recommandé de :

1. ne pas faire suivre ses messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles ;
2. ne pas héberger des données professionnelles sur des équipements personnels ou sur des moyens personnels de stockage en ligne ;
3. éviter de connecter des supports amovibles personnels aux ordinateurs de la structure professionnelle.

Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

Les données que l'on laisse sur Internet nous échappent instantanément. D'où la plus grande prudence dans la diffusion d'informations personnelles sur le Net.

Par exemple, en décochant les cases qui autoriseraient le site à conserver ou à partager ses données ou en utilisant plusieurs adresses électroniques dédiées à ses différentes activités (sérieuses ou autres) sur Internet.