Association Tunisienne de Prévention Positive | الجمعية التونسية للوقاية الايجابية

GUIDE DES BONNES MESURES DE LA SÉCURITÉ INFORMATIQUE

TABLE DES MATIERES

1

Choisir avec soin ses mots de passe

Dans le cadre de travail ou d'utilisation d'une adresse mail personnelle on peut choisir un mot de passe faible : 12345678. Ce mot de passe pourra être facilement reconstitué lors d'une attaque utilisant un outil automatisé : vous pouvez perdre de l'argent ou des données sensibles qui pourront être vendus.

Les mots de passe sont un moyen efficace de contrôler l'accès à vos données, aux appareils sur lesquels vous les stockez et aux services en ligne que vous utilisez. Cette page contient des conseils sur la façon de créer des mots de passe forts, comment s'en occuper et quoi faire si vous pensez qu'ils ont été volés.

Créer des mots de passe forts

Créer un fort et mémorable mot de passe pour votre compte de courriel (et d'autres comptes importants).

- Évitez d'utiliser des mots de passe prévisibles (comme des dates, des noms de famille et d'animaux). Évitez les mots de passe les plus courants que les criminels peuvent facilement deviner (comme 'passw0rd').

- Ne réutilisez pas le même mot de passe pour les comptes importants. Si un de vos mots de passe est volé, vous ne voulez pas que le criminel ait également accès (par exemple) à votre compte bancaire.

- Pour créer un mot de passe mémorable qui est également difficile à deviner, vous pouvez combiner trois mots au hasard pour créer un seul mot de passe (par exemple cupfishbiro).

Enregistrer vos mots de passe dans un endroit sécurisé

Si vous stockez vos mots de passe dans un endroit sûr, tu n'auras plus à te souvenir eux.

- Vous pouvez écrire vous mots de passe pour se souvenir, mais il faut les garder en lieu sûr,hors de vue, et (surtout) loin de votre ordinateur.

- Stockez vos mots de passe dans votre navigateur lorsque vous y êtes invité; c'est rapide, pratique et plus sûr que de réutiliser le même mot de passe. Les navigateurs peuvent également détecter les sites web 'douteux' que les e-mails de phishing essaient et vous trompent en visitant.

- Vous pouvez également utiliser un gestionnaire de mots de passe autonome pour vous aider à créer et à stocker des mots de passe forts.

Utiliser un 2FA pour protéger votre compte

Il s'appelle 2FAparce qu'il implique de se connecter à votre compte en utilisant deux mots de passe ou codes, l'un que vous connaissez, et l'autre généralement envoyé à votre téléphone.

- La forme la plus courante de 2FA est quand un code est envoyé à votre smartphone que vous devez entrer afin de procéder. On doit configurer 2FA pour les sites Web importants comme les services bancaires et les courriels.

- Même si un criminel connaît vos mots de passe, il aura de la difficulté à accéder aux comptes que vous avez protégés en activant 2FA.

- 2FA est supporté par des services en ligne populaires tels que Gmail, Facebook, Twitter, LinkedIn, Outlook et Instagram.

Que faire si votre mot de passe a été volé?

Si vous soupçonnez que votre mot de passe a été volé, vous devriez le modifier dès que possible.

- Si vous avez utilisé le même mot de passe sur d'autres comptes, modifiez-les également.
- Vous pouvez utiliser le site www.haveibeenpwned.com pour vérifier si vos renseignements ont déjà été rendus publics dans le cadre d'une atteinte majeure à la protection des données.

UN GESTIONNAIRE DE MOTS DE PASSE SÉCURISÉ ET GRATUIT

Ce petit logiciel libre et en français, certifié par l'ANSSI, permet de stocker en sécurité vos mots de passe pour les utiliser dans vos applications.
Il dispose aussi d'une fonction permettant de générer des mots de passe complexes aléatoires.
https ://keepass.info

2

Mettre à jour régulièrement vos logiciels

Si on ne met pas toujours à jour les logiciels on risque d'ouvrir une pièce jointe piégée sans s'apercevoir. Suite à cette erreur, des attaquants peuvent utiliser une vulnérabilité logicielle pénètrent l'ordinateur pour espionner les activités d'une organisation ou voler des données personnelles.

Les appareils numériques et les logiciels que nous utilisons au quotidien sont exposés à des failles de sécurité. Ces failles peuvent être utilisées par des cybercriminels pour prendre le contrôle d'un ordinateur, d'un équipement mobile ou encore d'une montre connectée. Face à ces risques, les éditeurs et les fabricants proposent des mises à jour (patch en anglais) visant à corriger ces failles. Si l'opération de mise à jour est souvent ressentie comme une contrainte, il s'agit pourtant d'un acte essentiel pour se protéger. Il convient donc, au sein de l'entreprise, de mettre en place certaines règles :

- **Pensez à mettre à jour sans tarder l'ensemble de vos appareils et logiciels**
  Ordinateurs, téléphones, systèmes d'exploitation, logiciels de traitement de texte, objets connectés… nous utilisons un grand nombre d'appareils et de logiciels. Il suffit qu'un seul ne soit pas à jour et soit exposé à une faille de sécurité pour ouvrir une brèche dans votre environnement numérique. Afin d'empêcher les cybercriminels d'utiliser ces failles de sécurité pour vous pirater et vous dérober des informations personnelles sensibles, il est primordial de réaliser les mises à jour de vos équipements dès qu'elles sont disponibles.

- **Téléchargez les mises à jour uniquement depuis les sites officiels**
  Seuls les sites ou dispositifs officiels des éditeurs et fabricants vous garantissent au mieux que les mises à jour que vous allez installer ne sont pas infectées par un virus. À l'installation de vos mises à jour, soyez attentif aux éventuelles conditions d'utilisation ou cases pré-cochées qui pourraient valoir acceptation de l'installation d'un autre logiciel non désiré (logiciels publicitaires, par exemple).

- **Activez l'option de téléchargement et d'installation automatique des mises à jour**
  Seuls les sites ou dispositifs officiels des éditeurs et fabricants vous garantissent au mieux que les mises à jour que vous allez installer ne sont pas infectées par un virus. À l'installation de vos mises à jour, soyez attentif aux éventuelles conditions d'utilisation ou cases pré-cochées qui pourraient valoir acceptation de l'installation d'un autre logiciel non désiré (logiciels publicitaires, par exemple).

3

LES SAUVEGARDES

On risque fort de perdu la totalité des fichiers clients ou internes de l'organisation suite à une panne d'ordinateur ou à une infection par un virus si on n'avait pas effectué de copie de sauvegarde.

Dans nos usages personnels ou professionnels, nous utilisons de nombreux appareils numériques pour créer et stocker des informations. Ces appareils peuvent cependant s'endommager ou être endommagés, entraînant une perte, parfois irréversible, de nos données. Afin de prévenir un tel risque, il est fortement conseillé d'en faire des copies pour préserver ces données à long terme.

- Effectuez des sauvegardes régulières de vos données
  En cas de perte, de vol, de panne, de piratage ou de destruction de vos appareils numériques, vous perdrez les données enregistrées sur ces supports. Il peut s'agir de données auxquelles vous accordez une importance particulière ou considérées comme essentielles dans le cadre de vos activités personnelles ou professionnelles (photos, vidéos, documents personnels ou de travail, etc.). Ayez le réflexe de réaliser régulièrement une sauvegarde de vos données.
- La plupart des solutions de stockage en nuage offrent un espace de stockage gratuit. Cela pourrait être suffisant pour enregistrer tous vos fichiers importants.
- Vous pouvez créer des sauvegardes basées sur le cloud automatiquement, ce qui signifie que vous êtes plus susceptible d'avoir une copie à jour de vos données.
- Le stockage en nuage nécessite une connexion Internet fiable, n'est donc pas adapté si le vôtre est lent, peu fiable ou mesuré.

- Protégez vos comptes cloud (et l'accès à vos sauvegardes) en utilisant des mots de passe forts et en activant l'authentification à deux facteurs (2FA).
- Les sauvegardes de supports amovibles peuvent contenir de grandes quantités de données, ce qui peut dépasser la capacité des options de stockage en nuage.
- Protégez votre sauvegarde avec un mot de passe fort en cas de perte ou de vol du support. Quelqu'un qui a les médias ne peut pas accéder à vos données à moins de connaître le mot de passe.

4

Installer un antivirus et sécuriser votre dispositif

Lors de la connexion d'un disque Usb, un virus a contamine le pc et incite l'utilisateur à formater le support informatique pour réutilisé son système d'exploitation ce qui a engendre une perte des données, et c'est à cause de l'absence d'un antivirus qui protège le dispositif .

Les virus sont un type de logiciel malveillant qui peut nuire aux appareils comme les ordinateurs, les ordinateurs portatifs, les téléphones intelligents et les tablettes.Une fois que votre appareil a été infecté, ce logiciel malveillant (aussi connu sous le nom de malware) peut voler vos données, l'effacer complètement, ou même vous empêcher d'utiliser votre appareil.

Les appareils peuvent être infectés en téléchargeant accidentellement une pièce jointe contenant des logiciels malveillants ou en branchant une clé USB déjà infectée. Vous pouvez même être infecté en visitant un site Web douteux.

Pour ces raisons, il est important que vous utilisiez toujours un logiciel antivirus sur vos ordinateurs portables et PC. Smartphones.

- Assurez-vous que votre produit audiovisuel est allumé et à jour. Windows et iOS ont des outils intégrés qui fournissent AV approprié.

- Les nouveaux ordinateurs sont souvent livrés avec une version d'essai d'un logiciel audiovisuel supplémentaire. Vous pouvez effectuer vos propres recherches pour savoir si ces produits sont bons pour vous.

- Assurez-vous que votre logiciel AV est configuré pour analyser automatiquement tous les nouveaux fichiers, tels que ceux téléchargés à partir d'Internet ou stockés sur une clé USB, un disque dur externe, une carte SD ou un autre type de support amovible.

- Vous n'avez pas besoin de produits audiovisuels sur votre téléphone intelligent ou votre tablette, à condition que vous n'installiez des applications que dans les magasins officiels.

- Téléchargez uniquement les applications pour smartphones et tablettes dans les magasins officiels (comme Google Play ou l'App Store). Les applications téléchargées des magasins officiels ont été vérifiées pour fournir une protection contre les virus et les logiciels malveillants.

- Si vous recevez un appel téléphonique offrant de l'aide pour supprimer les virus et les logiciels malveillants de votre ordinateur, raccrochez immédiatement (c'est une escroquerie).

5

Sécuriser l’accès Wi-Fi

La borne d’accès à Internet (box) d'une boutique est configurée pour utiliser le chiffrement WEP. Sans que le grant ne s’en aperçoive, un voisin a réussi en moins de deux minutes, à l’aide d’un logiciel, à déchiffrer la clé de connexion. Il a utilisé ce point d’accès Wi-Fi pour participer à une attaque contre un site Internet gouvernemental. Désormais, le grant est mise en cause dans l’enquête de police.*

L'utilisation du Wi-Fi est une pratique attractive. Il ne faut cependant pas oublier qu'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 réaliser des opérations malveillantes malintentionnées. Pour cette raison l'accès à Internet par un point d'accès Wi-Fi est à éviter dans le cadre de l'entreprise : une installation filaire reste plus sécurisée et plus performante.

Le Wi-Fi peut parfois être le seul moyen possible d'accéder à Internet, il convient dans ce cas de sécuriser l'accès en configurant votre borne d'accès à Internet. Pour ce faire :

- Dans l'interface de configuration de votre routeur , vérifiez que votre borne dispose du protocole de chiffrement WPA2 et activez-le. Sinon, utilisez la version WPA-AES (ne jamais utiliser le chiffrement WEP cassable en quelques minutes) ;
  - modifiez la clé de connexion par défaut (qui est souvent affichée sur l'étiquette de votre borne d'accès à Internet) par une clé (mot de passe) de plus de 12 caractères de types différents (cf. : 1-Choisissez des mots de passe robustes) ;
  - ne divulguez votre clé de connexion qu'à des tiers de confiance et changez la régulièrement ;
  - activez la fonction pare-feu de votre box ;
  - désactivez votre borne d'accès lorsqu'elle n'est pas utilisée.

- N'utilisez pas les Wi-Fi « publics » (réseaux offerts dans les gares, les aéroports ou les hôtels) pour des raisons de sécurité et de confidentialité ;

- Assurez-vous que votre ordinateur est bien protégé par un antivirus et un pare-feu. Si le recours à un service de ce type est la seule solution disponible (lors d'un déplacement, par exemple), il faut s'abstenir d'y faire transiter toute donnée personnelle ou confiden-tielle (en particulier messages, transactions financières). Enfin, il n'est pas recom-mandé de laisser vos clients, fournisseurs ou autres tiers se connecter sur votre réseau (Wi-Fi ou filaire).

- Préférez avoir recours à une borne d'accès dédiée si vous devez absolument fournir un accès tiers. Ne partagez pas votre connexion.

6

La sécurité des appareils mobiles

Un utilisateur possède un smartphone qu'il utilise à titre personnel comme professionnel. Lors de l'installation d'une application, il n'a pas désactivé l'accès de l'application à ses données personnelles. Désormais, l'éditeur de l'application peut accéder à tous les SMS présents sur son téléphone.

Bien que proposant des services innovants, les téléphones mobiles (smartphones) sont au-jourd'hui très peu sécurisés. Il est donc indispensable d'appliquer certaines règles élémentaires de sécurité informatique :

- N'installez que les applications nécessaires et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques…). Certaines applications demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement, il faut éviter de les installer ;

- En plus du code PIN qui protège votre carte téléphonique, utilisez un schéma ou un mot de passe pour sécuriser l'accès à votre terminal et le configurer pour qu'il se verrouille automatiquement ;
- Effectuez des sauvegardes régulières de vos contenus sur un support externe pour pouvoir les conserver en cas de restauration de votre appareil dans son état initial ;

- Chiffrez les données de l'appareil: En cas de perte ou de vol, seul le chiffrement des données contenues dans votre appareil vous assurera qu'une personne malintentionnée ne pourra contourner les codes d'accès et accéder quand même à vos informations. Tous les appareils récents proposent cette option qu'il suffit d'activer dans les paramètres et qui est quasi transparente à l'utilisation. Si vous utilisez une carte d'extension mémoire pour stocker vos informations, vérifiez qu'elle est également chiffrée.

- Ne stockez pas d'informations confidentielles sans protection: Ne notez jamais d'informations secrètes comme vos mots de passe ou vos codes bancaires dans votre répertoire de contacts, votre messagerie ou un fichier non chiffré sur votre appareil mobile. Un cybercriminel qui aurait pris le contrôle de votre appareil pourrait facilement les récupérer. En outre, certaines applications que vous avez installées peuvent aussi accéder et récupérer ces informations dont vous perdriez alors le contrôle. Pour protéger vos informations secrètes, utilisez une solution de chiffrement avec un mot de passe solide.

- Installer un vpn pour préserver votre anonymat.
- Installer une application de sécurité tel que Kaspersky mobile security.

7

Protéger ses données lors de ses déplacements

Dans un aéroport, un voyageur sympathise avec un autre prétendant avoir des connaissances en commun. Lorsque celui-ci lui demande s'il peut utiliser son ordinateur pour recharger son téléphone, le voyageur ne se méfie pas. L'inconnu en a profité pour exfiltrer les données concernant la mission professionnelle très confidentielle de voyageur.

L'emploi d'ordinateurs portables, des téléphones mobiles (smartphones) ou de tablettes faci-lite les déplacements professionnels ainsi que le transport et l'échange de données. Voyager avec ces appareils nomades fait cependant peser des menaces sur des infor-mations sensibles dont le vol ou la perte auraient des conséquences importantes sur les activités de l'organisation.

Avant de partir en mission

- N'utilisez que du matériel (ordinateur, supports amovibles, téléphone) dédié à la mission, et ne contenant que les données nécessaires ;
- Sauvegardez ces données, pour les retrouver en cas de perte ;
- Si vous comptez profiter des trajets pour travailler, emportez un filtre de protection écran pour votre ordinateur ;
- Apposez un signe distinctif (comme une pastille de couleur) sur vos appareils pour vous assurer qu'il n'y a pas eu d'échange pendant le transport ;
- Vérifiez que vos mots de passe ne sont pas préenregistrés.

Pendant la mission

- Gardez vos appareils, supports et fichiers avec vous, pendant votre voyage comme pendant votre séjour (ne les laissez pas dans un bureau ou un coffre d'hôtel) ;
- Désactivez les fonctions Wi-Fi et Bluetooth de vos appareils ;
- Retirez la carte SIM et la batterie si vous êtes contraint de vous séparer de votre téléphone ;
- N'utilisez pas les équipements que l'on vous offre si vous ne pouvez pas les faire vérifier par un service de sécurité de confiance ;
- Evitez de connecter vos équipements à des postes qui ne sont pas de confiance. Par exemple, si vous avez besoin d'échanger des documents lors d'une présenta-tion commerciale, utilisez une clé USB destinée uniquement à cet usage et effacez ensuite les données avec un logiciel d'effacement sécurisé ;

Après la mission

- Effacez l'historique des appels et de navigation ;
- Changez les mots de passe que vous avez utilisés pendant le voyage ;
- Faites analyser vos équipements après la mission, si vous le pouvez.
- N'utilisez jamais les clés USB qui peuvent vous avoir été offertes lors de vos déplace-ments.

8

Être prudent lors de l'utilisation de sa messagerie

Suite à la réception d'un courriel semblant provenir d'un de ses collègues, un internaute a cliqué sur un lien présent dans le message. Ce lien était piégé. Sans qu'il le sache, son ordinateur est désormais utilisé pour envoyer des courriels malveillants diffusant des images pornographiques.

Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées,etc.).

Lorsque vous recevez des courriels, prenez les précautions suivantes :

- l'identité d'un expéditeur n'étant en rien garantie : vérifiez la cohérence entre l'ex-péditeur présumé et le contenu du message et vérifier son identité. En cas de doute, ne pas hésiter à contacter directement l'émetteur du mail;
- n'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts;

- 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 située en bas à gauche de la fenêtre (à condition de l'avoir préalablement activée). Vous pour-rez ainsi en vérifier la cohérence;
- ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire). En effet, des courriels circulent aux couleurs d'institutions comme les Impôts pour récupérer vos données. Il s'agit d'attaques par hameçonnage ou « phishing »* ;

- n'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc. ;
- désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus* avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.

9

Télécharger ses programmes sur les sites officiels des éditeurs

Un internaute voulant se protéger des logiciels espions (spyware), a téléchargé un logiciel spécialisé proposé par son moteur de recherche. Sans le savoir, elle a installé un cheval de Troie.*

Si vous téléchargez du contenu numérique sur des sites Internet dont la confiance n'est pas assurée, vous prenez le risque d'enregistrer sur votre ordinateur des programmes ne pouvant être mis à jour, qui, le plus souvent, contiennent des virus ou des chevaux de Troie*. Cela peut permettre à des personnes malveillantes de prendre le contrôle à distance de votre machine pour espionner les actions réalisées sur votre ordinateur, voler vos données personnelles, lancer des attaques, etc.

Dans ce contexte, afin de veiller à la sécurité de votre machine et de vos données :

- téléchargez vos programmes sur les sites de leurs éditeurs ou d'autres sites de confiance ;
- pensez à décocher ou désactiver toutes les cases proposant d'installer des logiciels complémentaires ;
- restez vigilants concernant les liens sponsorisés et réfléchir avant de cliquer sur des liens ;
- désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus* avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.

10

Être vigilant lors d'un paiement sur Internet

Un administrateur a acheté sur Internet des fournitures de bureau pour son entreprise sans vérifier l'état de sécurité du site de commerce en ligne. Ce dernier n'était pas sécurisé. Des attaquants ont intercepté le numéro de carte bancaire de l'entreprise et l'ont utilisé pour passer des commandes en leur faveur.

Lorsque vous réalisez des achats sur Internet, via votre ordinateur ou votre ordi-phone (smartphone), vos coordonnées bancaires sont susceptibles d'être interceptées par des attaquants directement sur votre ordinateur ou dans les fichiers clients du site marchand. Ainsi, avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet :

- contrôlez la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs) ;
- assurez-vous que la mention « https:// » apparait au début de l'adresse du site Internet ;
- vérifiez l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'or-thographe par exemple.

Si possible, lors d'un achat en ligne :

- privilégiez la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS ;
- De manière générale, ne transmettez jamais le code confidentiel de votre carte bancaire ;
- n'hésitez pas à vous rapprocher votre banque pour connaître et utiliser les moyens sécurisés qu'elle propose.

11

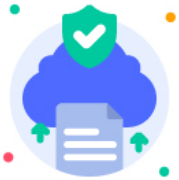
Séparer les usages personnels des usages professionnels

Un employé rapporte souvent du travail chez lui le soir. Sans qu'il s'en aperçoive son ordinateur personnel a été attaqué. Grâce aux informations qu'il contenait, l'attaquant a pu pénétrer le réseau interne de l'entreprise de l'employé. Des informations sensibles ont été volées puis revendues à la concurrence.

Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, ordiphone, etc.) personnels et professionnels.

Le AVEC (Apportez Votre Equipement personnel de Communication) ou BYOD (Bring Your Own Device) est une pratique qui consiste, pour les collaborateurs, à utiliser leurs équipements personnels (ordinateur, ordiphone, tablette, etc.) dans un contexte professionnel. Si cette solution est de plus en plus utilisée aujourd'hui, elle pose des problèmes en matière de sécurité des données (vol ou perte des appareils, intrusions, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur).

Dans ce contexte, il est recommandé de séparer vos usages personnels de vos usages professionnels :



- ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles ;
- n'hébergez pas de données professionnelles sur vos équipements personnels (clé USB, téléphone, etc.) ou sur des moyens personnels de stockage en ligne ;
- de la même façon, évitez de connecter des supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de l'entreprise.

Si vous n'appliquez pas ces bonnes pratiques, vous prenez le risque que des personnes malveillantes volent des informations sensibles de votre entreprise après avoir réussi à prendre le contrôle de votre machine personnelle.

12

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

Un internaute reçoit un courriel lui proposant de participer à un concours pour gagner un ordinateur portable. Pour ce faire, il doit transmettre son adresse électronique. Finalement, il n'a pas gagné mais reçoit désormais de nombreux courriels non désirés.

Les données que vous laissez sur Internet vous échappent instantanément.

Des personnes malveillantes pratiquent l'ingénierie sociale, c'est-à-dire récoltent vos informations personnelles, le plus souvent frauduleusement et à votre insu, afin de déduire vos mots de passe, d'accéder à votre système informatique, voire d'usurper votre identité ou de conduire des activités d'espionnage industriel.

Dans ce contexte, une grande prudence est conseillée dans la diffusion de vos informations personnelles sur Internet :

- soyez vigilant vis-à-vis des formulaires que vous êtes amenés à remplir :
  - » ne transmettez que les informations strictement nécessaires ;
  - » pensez à décocher les cases qui autoriseraient le site à conserver ou à partager vos données ;
- ne donnez accès qu'à un minimum d'informations personnelles et professionnelles sur les réseaux sociaux, et soyez vigilant lors de vos interactions avec les autres utilisateurs ;
- pensez à régulièrement vérifier vos paramètres de sécurité et de confidentialité ;
- enfin, utilisez plusieurs adresses électroniques dédiées à vos différentes activités sur Internet : une adresse réservée aux activités dites sérieuses (banques, recherches d'emploi, activité professionnelle…) et une adresse destinée aux autres services en ligne (forums, jeux concours…).

En résumé …

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

- désignez un correspondant/référent pour la sécurité informatique dans les entreprises ;
- rédigez une charte 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 et monitorez 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 aller plus loin

- https://www.ansi.tn
- http://www.ssi.gouv.fr
- https://www.ncsc.gov.uk/cyberessentials/overview
- https://gdpr-info.eu/
- https://security.web.cern.ch
- https://www.ontario.ca/fr/document/manuel-sur-lacces-linformation-et-la-protection-de-la-vie-privee

Glossaire

- **antivirus :** logiciel informatique destiné à identifier, neutraliser et effacer des logiciels malveillants ;
- **cheval de Troie :** programme qui s'installe de façon frauduleuse pour remplir une tâche hostile à l'insu de l'utilisateur (espionnage, envoi massif de spams,…) ;
- **chiffrement :** procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui ne possède pas la clé de (dé)chiffrement ;
- **compte d'administrateur :** compte permettant d'effectuer des modifications affectant les utilisateurs (modification des paramètres de sécurité, installer des logiciels…) ;
- **logiciel espion :** logiciel malveillant qui s'installe dans un ordinateur afin de collecter et transférer des données et des informations, souvent à l'insu de l'utilisateur.
- **Fournisseur d'Accès Internet (FAI) :** organisme (entreprise ou association) offrant une connexion à Internet ;
- **mise à jour :** action qui consiste à mettre à niveau un outil ou un service informatique en téléchargeant un nouveau programme logiciel ;
- **pare-feu (firewall) :** logiciel et/ou matériel permettant de protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet, protection d'un réseau d'entreprise,…) en filtrant les entrées et en contrôlant les sorties selon les règles définies par son utilisateur ;
- **paquet :** unité de transmission utilisée pour communiquer ;
- **phishing (hameçonnage) :** méthode d'attaque qui consiste à imiter les couleurs d'une institution ou d'une société (banque, services des impôts) pour inciter le destinataire à fournir des informations personnelles.
- **routeur :** élément intermédiaire dans un réseau informatique assurant la distribution des paquets de données en déterminant le prochain nœud de réseau auquel un paquet doit être envoyé ;
- **système d'exploitation :** logiciel qui, dans un appareil électronique, pilote les dispositifs matériels et reçoit des instructions de l'utilisateur ou d'autres logiciels ;

- **utilisateur :** personne qui utilise un système informatique ;
- **WEP :** protocole de sécurité permettant de fournir aux utilisateurs de réseaux locaux sans fil une protection contre le piratage ;
- **Wi Fi :** connexion Internet sans fil
- **WPA 2 :** standard de sécurité protégeant les utilisateurs contre le piratage des réseaux sans fil devant se substituer au système WEP jugé insuffisant.

Ce document a été élaboré comme un document de support relatif à l'ATELIER Renforcement des capacités dans le domaine de la sécurité numérique et la protection des données personnelles

Association Tunisienne de Prévention Positive
29 Rue Bichara Al Khouri, El Omrane
1005 Tunis - Tunisie

Tél : +216 71 896 901/ +216 71 896 023
Email : atpplus@atpplustunisie.com
Association Tunisienne De Prévention Positive
atp.plus