LA SÉCURITÉ NUMÉRIQUE ...

Pour vos fichiers, mais également pour vos informations personnelles

PRÉSENTATION DE INGLOBO

InGlobo est une agence web spécialisée dans l'accompagnement des artisans, commerçants et professions libérales. En plus de développer des sites internet et de créer des identités graphiques, InGlobo a développé des outils permettant aux petites structures de progresser dans les domaines de la vente, du marketing et bien sûr, de la communication sur internet.

Nous vous proposons ici le guide concernant la gestion de la sécurité numérique. La sécurité du numérique est l'affaire de tous. Elle repose avant tout sur des mesures simples et des bonnes pratiques à adopter sans modération dans la sphère privée et professionnelle. Fondées sur le bon sens, ces précautions élémentaires ne peuvent être négligées sans s'exposer à des risques, qui exploitent souvent des vulnérabilités connues.

Comme de nombreux artisans et commerçants qui nous ont déjà fait confiance, faites un pas décisif vers une meilleure rentabilité de votre commerce en vous dotant d'un site internet. Rendez-vous sur le site http://www.inglobo.fr et prenez connaissance de nos offres.

Découvrez nos points forts :

- Pas d'engagement de votre part tant que vous n'êtes pas satisfait du projet
- Un design unique pour vous, réalisé par des designers professionnels
- Des formules « tout compris » avec création du site + hébergement + nom de domaine + adresse mail professionnelle
- Des tarifs parmi les plus bas du marché

Nous sommes à votre écoute et vous pouvez nous poser toutes vos questions grâce au formulaire accessible par le lien : http://www.inglobo.fr/contact

Dans l'attente de vous retrouver sur notre site, nous vous souhaitons une agréable et instructive lecture.
Commercialement vôtre
L'équipe InGlobo

TABLE DES MATIÈRES

PRÉSENTATION DE INGLOBO 2
TABLE DES MATIÈRES 3
LA DÉFINITION DES RISQUES 4
LES BONNES PRATIQUES 7
1 Choisir avec soin ses mots de passe 7
2 Mettre à jour régulièrement vos logiciels 7
3 Bien connaître ses utilisateurs et ses prestataires 8
4 Effectuer des sauvegardes régulières 9
5 Sécuriser l'accès Wi-Fi de votre entreprise 9
6 Être aussi prudent avec son smartphone ou sa tablette qu'avec son ordinateur 10
7 Protéger ses données lors de ses déplacements 11
8 Être prudent lors de l'utilisation de sa messagerie 12
9 Télécharger ses programmes sur les sites officiels des éditeurs 12
10 Être vigilant lors d'un paiement sur Internet 13
11 Séparer les usages personnels des usages professionnels 13
12 Prendre soin de ses informations personnelles, professionnelles et de son identité numérique 14
En cas d'incident 15
Après l'incident 15
LE CAS DES ENFANTS 16
1 Internet, une interface avec le monde 16
2 Internet, une autre façon de tisser des liens 17
3 Internet, une cour de récréation planétaire 18
4 Internet, au bout du fil 19
CONCLUSION 20

LA DÉFINITION DES RISQUES

Avant de lister les bonnes pratiques, il nous a semblé intéressant de lister les menaces connues actuellement et qui peuvent rapidement causer de graves problèmes si l'on n'y prend garde.

Menaces	Descriptions
Virus (ou ver)	Un virus informatique se reproduit d'un fichier à un autre sur le même ordinateur. C'est le type de logiciel malveillant Internet le plus ancien et le plus répandu. Les formes de virus évoluent sans arrêt. Il est donc important de se tenir informé des derniers risques en la matière. Généralement, si vous disposez d'un antivirus (AVAST par exemple), et que vous le mettez à jour régulièrement (ou avez paramétré les mises à jour régulières), vous devriez avoir un premier niveau de protection efficace.
Ver informatique (worm)	Un ver informatique (worm en anglais) ne se reproduit pas d'un fichier à un autre mais d'un ordinateur à un autre, via un réseau local ou le réseau Internet.
Cheval de Troie (trojan)	Un cheval de Troie (trojan en anglais) cache un logiciel malveillant, appelé charge utile, dans un autre programme parfaitement sain. L'usage le plus fréquent d'un cheval de Troie est d'installer sur un ordinateur victime une porte dérobée (backdoor) pour pouvoir y revenir plus tard, ou un keylogger : voir ci-dessous. Le contrôle à distance permet à un pirate situé n'importe où dans le monde de manipuler votre ordinateur presque comme si il était à votre place : lancer des programmes, ouvrir des dossiers, vous envoyer des messages en pop-up, etc ... Indépendamment du piratage, le contrôle à distance est aussi utilisé pour de la maintenance informatique normale. Souvent intégré dans un troyen, un keylogger permet d'espionner votre frappe au clavier.

Porte dérobée (backdoor)	Une porte dérobée (backdoor en anglais) est un moyen d'accès caché à un ordinateur, à distance et discrétement, pour y exécuter toutes sortes d'actions nuisibles prévues par ce programme. Autrement dit une porte dérobée permet d'accéder à un ordinateur distant sans que son utilisateur s'en aperçoive. Comme action nuisible, il est possible de lire les fichiers de l'ordinateur distant, les modifier, les supprimer, et d'installer n'importe quel programme malveillant. Comme exemple de logiciel malveillant Internet de ce type, on trouve un serveur de spam ou un programme de saturation de site Web. L'ordinateur infecté devient nuisible à l'insu de son utilisateur : on appelle cela un zombie.
Keylogger (enregistreur de frappe)	Un keylogger enregistre toutes les touches frappées au clavier sur l'ordinateur infecté, et les envoie au pirate sur Internet (par exemple par email). Souvent le but est d'intercepter les pseudonymes et mots de passe de la victime sur des sites Web, pour usurper son "identité virtuelle", voire voler son argent sur des sites financiers (banque, enchères en ligne ...).
Rootkit (programme invisible)	Un rootkit est un programme qui en cache un autre aux yeux de l'utilisateur de l'ordinateur. Il n'est pas nuisible en tant que tel, mais souvent utilisé à des fins malveillantes.
Spyware (logiciel espion)	Un spyware, ou logiciel espion, enregistre les habitudes de navigation sur le Web de l'utilisateur, si possible avec ses coordonnées, et les envoie à un destinataire peu respectueux de la vie privée des internautes. Tout est fait à l'insu de l'internaute.
Le phishing primaire et secondaire	Un rogue est un faux antivirus ou un faux anti-spyware, qui se manifeste sous la forme d'une fenêtre publicitaire qui s'ouvre sans arrêt, prévenant d'une soi-disante infection, et propose à l'utilisateur de télécharger un programme payant pour "désinfecter" l'ordinateur. La fenêtre publicitaire s'ouvre régulièrement jusqu'à ce que la victime achète le faux antivirus. Un rogue est une arnaque.
Dialer (composeur de numéro de téléphone)	Un dialer (composeur de numéro de téléphone) est un programme malveillant cherchant à composer un numéro de téléphone surtaxé sur votre modem téléphonique. Le pirate est rémunéré par une commission sur le prix de l'appel surtaxé. Les dialers ne marchent que sur des modems RTC, utilisant le bon vieux signal classique RTC de la ligne téléphonique

RansomWare : logiciel rançonneur	Un RansomWare est un logiciel rançonneur cryptant certains fichiers sur l'ordinateur de la victime. Le rançonneur propose la clé de décryptage contre de l'argent, autrement dit pour récupérer ses fichiers il faut payer une rançon. On peut citer Lorobot et Gpcode comme spécimens de ce type de menace.
Hijacker : pirate de navigateur	Un Hijacker est un pirate de navigateur qui cherche à vous faire visiter un ou plusieurs sites Web particuliers. Il modifie un paramètre du navigateur, tel que la page de démarrage, les favoris ou la page de recherche. Cela paraît facile à corriger mais un haijacker fait souvent en sorte de bloquer ou d'annuler la correction, en remodifiant le paramètre au démarrage du système, par exemple.
Les cookies confidentiels	Un cookie contient des informations utiles, et un cookie confidentiel représente un risque faible de traçage et de piratage. Les cookies d'authentification identifient chaque abonné d'un service Web, qu'il s'agisse du pseudonyme et du mot de passe, ou le numéro de votre session. Un cookie enregistré par un site ne peut être lu par un autre, mais un programme pirate peut voler le cookie d'un abonné au service sous certaines conditions. Vous avez la possibilité sur votre navigateur, de choisir de ne pas enregistrer les cookies. Votre navigation sera peut-être un peu plus fastidieuse (il vous faudra retaper certaines informations régulièrement), mais en tout cas, surement plus sure !!!

LES BONNES PRATIQUES

1 Choisir avec soin ses mots de passe

Le mot de passe est un outil d'authentification utilisé notamment pour accéder à un équipement numérique et à ses données. Pour bien protéger vos informations, choisissez des mots de passe difficiles à retrouver à l'aide d'outils automatisés ou à deviner par une tierce personne.

Choisissez des mots de passe composés si possible de 12 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec vous (nom, date de naissance…) et ne figurant pas dans le dictionnaire.

Deux méthodes simples peuvent vous aider à définir vos mots de passe

- *La méthode phonétique* : « J'ai acheté 5 CDs pour cent euros cet après-midi » :
  - ght5CDs%E7am
- *La méthode des premières lettres* : « Allons enfants de la patrie, le jour de gloire est arrivé » :
  - aE2lP,lJ2Géa!

Définissez un mot de passe unique pour chaque service sensible. Les mots de passe protégeant des contenus sensibles (banque, messagerie professionnelle…) ne doivent jamais être réutilisés pour d'autres services.

Il est préférable de ne pas recourir aux outils de stockage de mots de passe. A défaut, il faut s'en tenir à une solution ayant reçu une certification de premier niveau (CSPN)

En entreprise :

- Déterminez des règles de choix et de dimensionnement (longueur) des mots de passe et faites les respecter ;
- Modifiez toujours les éléments d'authentification (identifiants, mots de passe) définis par défaut sur les équipements (imprimantes, serveurs, box…) ;
- Rappelez aux collaborateurs de ne pas conserver les mots de passe dans des fichiers ou sur des post-it ;
- Sensibilisez les collaborateurs au fait qu'ils ne doivent pas préenregistrer leurs mots de passe dans les navigateurs, notamment lors de l'utilisation ou la connexion à un ordinateur public ou partagé (salons, déplacements…).

2 Mettre à jour régulièrement vos logiciels

Dans chaque système d'exploitation (Android, IOS, MacOS, Linux, Windows,…), logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées par les éditeurs qui proposent alors aux utilisateurs des mises à jour de sécurité. Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations encore longtemps après leur découverte et leur correction.

Il convient donc, au sein de l'entreprise, de mettre en place certaines règles :

- Définissez et faites appliquer une politique de mises à jour régulières
- S'il existe un service informatique au sein de l'entreprise, il est chargé de la mise à jour du système d'exploitation et des logiciels
- S'il n'en existe pas, il appartient aux utilisateurs de faire cette démarche, sous l'autorité du chef d'entreprise
- Configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible. Sinon, téléchargez les correctifs de sécurité disponibles
- Utilisez exclusivement les sites Internet officiels des éditeurs

3 Bien connaître ses utilisateurs et ses prestataires

Lorsque vous accédez à votre ordinateur, vous bénéficiez de droits d'utilisation plus ou moins élevés sur celui-ci. On distingue généralement les droits dits «d'utilisateur» et les droits dits «d'administrateur».

- Dans l'utilisation quotidienne de votre ordinateur (naviguer sur Internet, lire ses courriels, utiliser des logiciels de bureautique, de jeu,…), prenez un compte utilisateur. Il répondra parfaitement à vos besoins.
- Le compte administrateur n'est à utiliser que pour intervenir sur le fonctionnement global de l'ordinateur (gérer des comptes utilisateurs, modifier la politique de sécurité, installer ou mettre à jour des logiciels,…).

Les systèmes d'exploitation récents vous permettent d'intervenir facilement sur le fonctionnement global de votre machine sans changer de compte : si vous utilisez un compte utilisateur, le mot de passe administrateur est demandé pour effectuer les manipulations désirées. Le compte administrateur permet d'effectuer d'importantes modifications sur votre ordinateur.

Au sein de l'entreprise :

- Réservez la gestion de vos ordinateurs au service informatique, si celui-ci existe
- Dans le cas contraire, protégez-en l'accès, n'ouvrez pour les employés que des comptes utilisateur, n'utilisez pas le compte administrateur pour de la navigation sur Internet
- Identifiez précisément les différents utilisateurs du système et les privilèges qui leur sont accordés. Tous ne peuvent pas bénéficier de droits d'administrateur
- Supprimez les comptes anonymes et génériques (stagiaire, contact, presse, etc.). Chaque utilisateur doit être identifié nommément afin de pouvoir relier une action sur le système à un utilisateur
- Encadrez par des procédures déterminées les arrivées et les départs de personnel pour vous assurer que les droits octroyés sur les systèmes d'information sont appliqués au plus juste et surtout qu'ils sont révoqués lors du départ de la personne.

4 Effectuer des sauvegardes régulières

Pour veiller à la sécurité de vos données, il est vivement conseillé d'effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires par exemple). Vous pourrez alors en disposer suite à un dysfonctionnement de votre système d'exploitation ou à une attaque.

Pour sauvegarder vos données, vous pouvez utiliser des supports externes tels qu'un disque dur externe réservé exclusivement à cet usage, ou, à défaut, un CD ou un DVD enregistrable que vous rangerez ensuite dans un lieu éloigné de votre ordinateur, de préférence à l'extérieur de l'entreprise 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 contenant les données d'origine. Néanmoins, il est nécessaire d'accorder une attention particulière à la durée de vie de ces supports.

Nota : sachez qu'il existe un type de disque très intéressant pour cela. Il s'agit des disques NAS disposant un port Ethernet, et qui peuvent se brancher directement sur votre box. A partir de là, vous pouvez y accéder de n'importe quel appareil soit en WiFi, soit via une liaison CPL, soit en étant relié par cable à votre box.

Avant d'effectuer des sauvegardes sur des plateformes sur Internet (souvent appelées « cloud » ou « informatique en nuage »), soyez conscient que ces sites de stockage peuvent être la cible d'attaques informatiques et que ces solutions impliquent des risques spécifiques :

- Risques pour la confidentialité des données,
- Risques juridiques liés à l'incertitude sur la localisation des données,
- Risques pour la disponibilité et l'intégrité des données,
- Risques liés à l'irréversibilité des contrats.

Pour vous prémunir, voici quelques conseils :

- Soyez vigilant en prenant connaissance des conditions générales d'utilisation de ces services. Les contrats proposés dans le cadre des offres génériques ne couvrent généralement pas ces risques ;
- Autant que possible, n'hésitez pas à recourir à des spécialistes techniques et juridiques pour la rédaction des contrats personnalisés et appropriés aux enjeux de votre entreprise ;
- Veillez à la confidentialité des données en rendant leur lecture impossible à des personnes non autorisées en les chiffrant à l'aide d'un logiciel de chiffrement avant de les copier dans le « cloud ».

5 Sécuriser l'accès Wi-Fi de votre entreprise

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, n'hésitez pas à contacter l'assistance technique de votre fournisseur d'accès. Les fournisseurs d'accès à Internet vous guident dans cette configuration en vous proposant différentes étapes, durant lesquelles vous appliquerez ces recommandations de sécurité :

- Au moment de la première connexion de votre ordinateur en Wi-Fi, ouvrez votre navigateur Internet pour configurer votre borne d'accès. L'interface de configuration s'affiche dès l'ouverture du navigateur. Dans cette interface, modifiez l'identifiant de connexion et le mot de passe par défaut qui vous ont été donnés par votre fournisseur d'accès
- Dans cette même interface de configuration, que vous pouvez retrouver en tapant l'adresse indiquée par votre fournisseur d'accès, 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. : Choisissez des mots de passe robustes dans la section précédente)
- 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 confidentielle (en particulier messages, transactions financières). Enfin, il n'est pas recommandé 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 Être aussi prudent avec son smartphone ou sa tablette qu'avec son ordinateur

Bien que proposant des services innovants, les smartphones sont aujourd'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

- Ne préenregistrez pas vos mots de passe

7 Protéger ses données lors de ses déplacements

L'emploi d'ordinateurs portables, de smartphones ou de tablettes facilite les déplacements professionnels ainsi que le transport et l'échange de données. Voyager avec ces appareils nomades fait cependant peser des menaces sur des informations 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 ;
- Informez votre entreprise en cas d'inspection ou de saisie de votre matériel par des autorités étrangères
- 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 présentation commerciale, utilisez une clé USB destinée uniquement à cet usage et effacez ensuite les données avec un logiciel d'effacement sécurisé
- Refusez la connexion d'équipements appartenant à des tiers à vos propres équipements (smartphone, clé USB, baladeur…)

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 déplacements (salons, réunions, voyages…) : très prisées des attaquants, elles sont susceptibles de contenir des programmes malveillants.

8 Être prudent lors de l'utilisation de sa messagerie

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'expéditeur 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 pourrez 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

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

Lorsque vous réalisez des achats sur Internet, via votre ordinateur ou votre 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'orthographe 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

Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, smartphone, 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, smartphone, 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

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 cas d'incident

Vous n'avez pas eu le temps de mettre en œuvre les règles décrites dans ce guide ou les attaquants ont réussi à les contourner. Ne cédez pas à la panique, et ayez les bons réflexes.

- En cas de comportement inhabituel de votre ordinateur, vous pouvez soupçonner une intrusion (impossibilité de se connecter, activité importante, connexions ou activités inhabituelles, services ouverts non autorisés, fichiers créés, modifiés ou supprimés sans autorisation,…)
- Déconnectez la machine du réseau, pour stopper l'attaque. En revanche, maintenez-là sous tension et ne la redémarrez pas, pour ne pas perdre d'informations utiles pour l'analyse de l'attaque
- Prévenez votre hiérarchie, ainsi que le responsable de la sécurité, au téléphone ou de vive voix, car l'intrus peut-être capable de lire les courriels. Prenez également contact avec un prestataire informatique qui vous aidera dans la restauration de votre système ainsi que dans l'analyse de l'attaque
- Faites faire une copie physique du disque
- Faites rechercher les traces disponibles liées à la compromission. Un équipement n'étant jamais isolé dans un système d'information, des traces de sa compromission doivent exister dans d'autres équipements sur le réseau (pare-feu, routeurs, outils de détection d'intrusion, etc.)
- Déposez une plainte auprès de la brigade de gendarmerie ou du service de police judiciaire compétent pour le siège de la société, de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (Paris et petite couronne), ou de la Direction générale de la sécurité intérieure

Après l'incident

- Réinstallez complètement le système d'exploitation à partir d'une version saine, supprimez tous les services inutiles, restaurez les données d'après une copie de sauvegarde non compromise, et changez tous les mots de passe du système d'information.

LE CAS DES ENFANTS

1. Internet, une interface avec le monde

Surf, Recherche d'informations, Téléchargement

A la maison, c'est plus convivial de vivre tous ensemble plutôt que chacun derrière son écran !

- Mettez l'ordinateur dans un espace de vie commun, pas dans la chambre des enfants. Et jusqu'à un certain âge faites en sorte qu'ils demandent la permission avant de se connecter.
- Comment font-ils leurs recherches d'information sur le web, ont-ils une stratégie pour choisir leurs sites, leurs mots clés ?

Tout n'est pas toujours vrai sur Internet.

- Vos enfants doivent apprendre à développer un esprit critique, à recouper leurs sources, et à éviter le copier-coller sauvage. Evaluer la fiabilité des sites est complexe : votre regard critique peut se révéler précieux.
- Ils ont un baladeur, écoutent de la musique ou regardent des films en ligne. Connaissent-ils les lois sur le téléchargement ?
  - On peut télécharger tout à fait légalement. Mais pas tout.
- Les téléchargements gratuits de musique ou vidéo par les systèmes « peer to peer » sont rarement autorisés et peuvent aussi être sources de virus. Le piratage est puni par la loi. En revanche, il existe des sites tout à fait légaux où découvrir tous les nouveaux morceaux en streaming (sans les télécharger).

Est-ce vraiment gratuit ?

- Il existe de nombreux sites de jeux gratuits. Vraiment gratuits?
  - Certains le sont, d'autres se rétribuent en vendant les données personnelles fournies par les utilisateurs : invitez vos enfants, avant de donner des informations sur des sites, à lire la politique de ceux-ci en matière de protection et utilisation de données, et de façon plus générale à décocher la case "offres partenaires".

Comment remplir un formulaire ?

- Sur la plupart des formulaires que l'on rencontre sur Internet, tous les champs ne doivent pas forcément être remplis.
- Seuls ceux qui ont un astérisque sont obligatoires. Pour les autres, autant réfléchir avant de les renseigner.

Leur est-il arrivé de voir des images qui choquent ou font peur ?

- En cas de soucis, dites-leur d'éteindre l'écran et de vous en parler.
- Des logiciels de contrôle parental sont disponibles gratuitement auprès de votre fournisseur d'accès : pensez à en installer un.

Bien surfer, ça s'apprend

2. Internet, une autre façon de tisser des liens

Chat, forums, Blog, Réseaux sociaux, Messageries

Un écran n'agit pas comme une cage d'invisibilité

- Même avec un pseudo, vos enfants doivent savoir que surfer laisse des traces : adresse IP, historique de navigation, mots clés saisis dans un moteur de recherche, etc.
- Sur certains sites, des logiciels publicitaires étudient aussi les clics effectués pour proposer des contenus "ciblés".
- Un blog, c'est comme un journal : ce qu'on y publie est vu par tout le monde, pendant très longtemps
- Le blog n'est pas un journal intime. Vos enfants doivent être conscients que ce qu'ils y publient part sur la voie publique et qu'ils en sont responsables légalement.
- Avant de publier une photo d'amis (ou de professeurs), il faut demander leur autorisation ou celle de leurs parents s'ils sont mineurs.
- Lorsqu'ils postent une photo/vidéo d'eux-mêmes, ils feraient bien aussi de se demander s'ils seront contents que tout le monde puisse la voir, et ceci pendant des années. MySpace, Facebook… les réseaux sociaux ont leurs propres modes d'emploi. Faciles d'utilisation, ces plateformes ne sont pas forcément configurées par défaut pour mieux protéger la vie privée.
- Prenez le temps de vous assurer que vos enfants maîtrisent les outils mis à leur disposition sur ces sites : les options associées à leur profil permettent de ne pas donner toutes leurs informations à tout le monde, ou de cibler la diffusion de leurs activités à certains membres choisis de leurs réseaux seulement.
- Apprenez-leur à sélectionner les groupes auxquels ils souhaitent appartenir. Ou pas. Avoir des centaines d'amis virtuels, qu'est-ce que cela signifie vraiment ?
- Sur les messageries instantanées ou les réseaux sociaux, comme dans la cour de récréation, la cote de popularité se mesure parfois au nombre d'amis que l'on peut afficher. Là aussi, pourtant, il faut apprendre à choisir ses amis : vous pouvez par exemple vérifier avec votre enfant qu'il n'accepte pas comme amis des gens qu'il ne connaît pas dans la vie réelle.
- S'ils veulent rencontrer quelqu'un connu sur Internet, il est impératif qu'ils en parlent à un adulte et aillent au rendez-vous accompagné. Qui est derrière la souris, on ne peut pas toujours savoir. C'est la raison pour laquelle il ne faut communiquer sur Internet ni son nom, adresse ou numéro de téléphone, ni le nom de son école ou de son club de sport, et contrôler ses contacts dans les chats ou les réseaux sociaux.

Communiquer, ça s'apprend

3. Internet, une cour de récréation planétaire

Jeux en ligne

Connaissent-ils les significations des symboles du PEGI, le système de classification des jeux vidéo ?

- A chaque jeu son âge. Ce qui est bon pour l'un de vos enfants ne l'est pas forcément pour son petit frère ou sa petite sœur… Ceci étant, les aînés sont souvent de bon conseil pour déterminer les activités adaptés aux plus jeunes.
- A chaque enfant sa maturité aussi : mieux vaut tester soi-même les jeux de ses enfants pour s'assurer qu'ils leur conviennent bien.
- Ils jouent beaucoup en ligne. Ont-ils encore assez de temps pour voir leurs amis et avoir d'autres passions ?
- Nombre d'heures, type de jeu… pour l'utilisation d'Internet comme le reste, il faut fixer des règles et s'y tenir. Mais lesquelles ? Pour aider vos enfants à mieux gérer leur temps, il convient de connaître les jeux qu'ils pratiquent, qui ne se prêtent pas forcément tous aux mêmes règles.
- Certains jeux peuvent ne prendre que quelques instants et se jouer en solo. On peut les arrêter à pratiquement tout moment.
- D'autres se jouent en équipe, parfois pour des parties assez longues que l'on ne peut arrêter en cours. Eteindre l'ordinateur pour aller diner est alors plus difficile, dans la mesure où cela peut pénaliser le reste de l'équipe.
- D'autres jeux encore ne s'arrêtent jamais et récompensent le temps passé sur l'ordinateur autant que le talent du joueur...

L'essentiel est donc de jouer avec votre enfant, de lui apprendre tôt à gérer son temps, de fixer des limites…

AGE > Age conseillé

VIOLENCE > Jeu contenant des scènes violentes

GROSSIÈRETÉ > Jeu contenant des expressions vulgaires

PEUR > Jeu dont le contenu peut effrayer de jeunes enfants

SEXE > Jeu montrant la nudité et/ou contacts sexuels ou faisant allusion au sexe

DROGUES > Jeu faisant référence aux drogues ou montrant leur usage

DISCRIMINATION > Jeu montrant ou encourageant la discrimination

JEUX DE HASARD > Jeu qui encourage ou enseigne les jeux de hasard

Certains jeux sont dotés d'un système de contrôle parental, habituellement activable lors de l'installation, qui permet de limiter les temps de jeux à des plages horaires autorisées. Renseignez-vous

Jouer, ça s'apprend

4. Internet, au bout du fil

Téléphonie mobile

Internet sur Mobile répond aux mêmes règles que sur un ordinateur.

- Les logiciels de contrôle parental sont aussi offerts par tous les opérateurs mobiles. Des copains harcelés par mail et sur portable, ça arrive, ça peut aussi s'arrêter. Des messages anonymes sur ses messageries fixes ou mobiles, via SMS, sur son blog… les nouveaux médias facilitant l'anonymat peuvent encourager ce type de pratiques perturbantes. L'essentiel est ici d'aider les jeunes à briser le silence, à en parler à leurs amis et aux adultes, et leur éviter de culpabiliser.
- Leur rappeler, encore, qu'il ne faut pas donner son numéro de portable à n'importe qui, ni dans la cour de récré, ni sur Internet.

- Certains sites proposent de payer des produits, par exemple des sonneries de téléphone ou des jeux, en donnant son numéro de téléphone mobile. Mieux vaut vérifier que le site en question est un site sérieux. Et ce qu'il en coûtera !

- Oreillettes, utilisation sur la voie publique ou en scooter, temps passé au téléphone... veillez à ce que l'usage du mobile par votre enfant se fasse dans les meilleures conditions.

La mobilité, ça s'apprend

CONCLUSION

Félicitation ! Vous arrivez au terme de ce guide sur la sécurité numérique.

Nous espérons que vous pourrez maintenant vous assurer que vos données sont en sécurité. N'oubliez pas que lorsque l'on parle de vos données, cela peut être bien évidemment vos fichiers et autres informations de ce type, mais également, les données qui vous caractérisent en terme de personne (identité …).

Rien n'est jamais perdu dans le monde internet et nombreux sont ceux qui ont eu la surprise de voir s'afficher des données les concernant qu'ils pensaient avoir détruites ou oubliées !!! Donc, réfléchissez à deux fois avant de poster des informations personnelle sur internet (même, voire peut-être surtout) si vous vous trouvez sur une page d'un réseau social !

Gardez en tête que cette démarche n'est jamais figée dans le temps. Soyez à l'écoute des informations concernant la sécurité des données et mettez à jour vos façons de faire en fonction des nouveaux risques qui vont surement arriver dans les mois / années à venir.

Nous espérons en tout cas vous avoir donné les bases de réflexion pour vous protéger au mieux à l'avenir.

Avec InGlobo, vous n'êtes plus seul face à internet !

Commercialement vôtre
L'équipe InGlobo