Respecter et faire respecter les recommandations de sécurité

SECURISER UN EQUIPEMENT NUMERIQUE MOBILE

1 INTRODUCTION

Le gros avantage des Smartphones, iPhone et autres tablettes est leur «mobilité» mais cela induit des risques et donc, des précautions spécifiques.

2 REGLES DE BONNE CONDUITE CONCERNANT VOTRE MOBILE

2.1 Méfiez-vous des regards indiscrets

Ne laissez pas trainer votre téléphone, gardez le sur vous.

Dans tout lieu public, une personne malveillante attentive pourrait mémoriser des données affichées à l'écran ou les touches du clavier que vous utilisez pour entrer un code confidentiel.

2.2 Prévoyez le vol ou de la perte de votre appareil

Si votre appareil contient des données confidentielles en clair (dont des identifiants et mots de passe), ces informations pourraient être utilisées à votre détriment.

Il est donc conseillé de **crypter les données sensibles** et de **protéger votre écran de verrouillage par un mot de passe**, même si on perd un peu en facilité d'utilisation.

Pensez à **sauvegarder vos données**, la plupart des opérateurs téléphoniques propose des espaces en mode SAS pour les sauvegardes. En cas de perte ou de panne cela sera bien utile.

Certaines applications permettent d'activer le verrouillage du téléphone ou d'effacer les données à distance, utile en cas de vol.

D'autres applications permettent de localiser votre mobile, ce qui peut vous aider à le retrouver en cas de perte.

Respecter et faire respecter les recommandations de sécurité

2.2.1 IMEI : International Mobile Equipment Identity

Ce numéro permet à l'opérateur du réseau d'identifier le mobile appelant et ainsi de l'autoriser ou non à se connecter. Ce code permet de pouvoir bloquer un mobile volé auprès de l'ensemble des opérateurs.

Il est donc très important de noter ce numéro qui se trouve sur votre contrat d'abonnement ou sur la boite de votre téléphone. Si vous ne disposez pas du contrat ou de la boite, vous pouvez aussi composer le ***#06#** sur votre mobile, ou en faire la demande auprès de votre opérateur. Cela vous sera utile en cas de perte ou de vol de votre téléphone.

2.2.2 PIN: Numéro d'Identification Personnel

Le code PIN 1, est utilisé par tous, il permet de sécuriser l'accès à la carte SIM, et au réseau. Il vous est fourni avec votre carte SIM.
En cas d'erreur, à 3 reprises, le téléphone est verrouillé et demande un **code PUK** pour le réactiver. Ce code PUK est disponible dans les documents fournis à l'achat du mobile, en appelant votre opérateur ou sur son site internet. Il a cependant ses limites et sera insuffisant en cas de vol de votre téléphone allumé. En effet, un téléphone dérobé allumé peut être utilisé et donne accès aux données sensibles.

Le code PIN 2 protège l'accès à certaines fonctionnalités de votre mobile, par exemple il peut bloquer l'accès à votre répertoire. Pour obtenir votre code PIN 2, contactez votre service clients ou regardez le manuel de votre téléphone.

2.3 Gestion des fonctions Bluetooth

Si ces fonctions apportent une souplesse d'utilisation importante (écouteur sans fil, etc.), elles peuvent être utilisées à vos dépens. Dans un environnement peuplé (aéroport, train, embouteillage, etc.), la désactivation des fonctions Bluetooth™ est recommandée. De façon générale, n'activez les fonctions Bluetooth™ que lorsque c'est nécessaire.

2.4 Gestion des fonctions WiFi

Lorsque vous utilisez ce type de connexion, veillez à n'y faire circuler des informations sensibles (connexion avec votre banque, par exemple) que si la connexion est sécurisée (WPA2, filtrage Mac). La désactivation des fonctions WI-FI est recommandée, de façon générale, n'activez les fonctions WiFi, que lorsque c'est nécessaire.

Respecter et faire respecter les recommandations de sécurité

3 PRECAUTIONS CONCERNANT LES LOGICIELS MALVEILLANTS

Un smartphone ou un iPhone™ est un véritable ordinateur avec sensiblement les mêmes possibilités mais aussi les mêmes faiblesses, en particulier concernant les logiciels malveillants tels que virus, chevaux de Troie, logiciels espion, etc... D'où les recommandations suivantes.

3.1 Pour les smartphones

Pour éviter les failles de sécurité, effectuez les mises à jour du système d'exploitation au fur et à mesure de leur mise à disposition sur le site Web du constructeur.

Installez un **antivirus** pour mobile et tenez à jour régulièrement sa base de signatures.

Comme sur un PC, n'ouvrez pas les pièces jointes reçues dans un mail d'expéditeur inconnu.

3.2 Pour les iPhones

Connecter régulièrement votre iPhone™ au serveurs Apple afin de télécharger les éventuelles mises à jour du système d'exploitation.

Ne pas « jailbreaker » l'équipement (le « jailbreak » permet de contourner les protections de l'iPhone™ pour installer des applications autres que celles disponibles sur le site « Apple Store »).

Respecter et faire respecter les recommandations de sécurité

4 UTILISATION D'APPAREILS NE VOUS APPARTENANT PAS

Par exemple un téléphone d'un ami ou un équipement d'un cybercafé dont vous ne maîtrisez pas le niveau de protection.

Etant donné que vous ne maîtrisez pas l'équipement informatique, la saisie d'informations personnelles, bancaires ou confidentielles pourrait être capturée (par un virus par exemple). De plus, comme tout utilisateur d'un ordinateur/téléphone/PDA laisse des traces de son activité, une autre personne pourrait avoir accès à des informations comme votre navigation sur Internet, les sites consultés, les numéros appelés, etc...

Sur des appareils ne vous appartenant pas, les règles de bonne conduite conseillées sont de ne pas effectuer d'opérations sensibles telles que : visualiser vos comptes bancaires en ligne, effectuer des achats en ligne ou toute autre opération nécessitant la saisie d'informations confidentielles.

Respecter et faire respecter les recommandations de sécurité

5 MOBILES D'ENTREPRISE :

Dans le cadre de l'entreprise, on distingue 2 catégories de terminaux mobiles :

- Ceux fournis par l'entreprise
- Ceux qui appartiennent personnellement aux employés et qui sont employés à la fois dans le cadre privé et dans le cadre du travail. C'est le phénomène du **BYOD** (Bring Your Own Device)

Les données de l'entreprise circulent en toute liberté, souvent non surveillées La mobilité génère de nouveaux risques qui n'existent pas dans un mode fixe.

Un collaborateur ciblé peut se voir géo localisé, pisté, écouté. On peut lui voler son terminal, y insérer un mouchard, prendre son contrôle à distance et lui dérober des données.

Les informations ne se trouvant plus uniquement dans l'enceinte de l'entreprise disponible aux heures ouvrables, il faut trouver un moyen de la préserver en permanence et partout.

5.1 Aspect technique

La perméabilité entre vie privée et vie professionnelle et la mobilité des terminaux mobiles imposent à l'entreprise des outils pour couvrir les risques identifiés.

L'offre de sécurité est de 3 types.

5.1.1 Mobile Device Management (MDM)

Une application MDM ou "Gestion de Terminaux Mobiles", est une application permettant la gestion d'une flotte d'appareils mobiles depuis le système d'information de l'entreprise. Cela peut aller d'une flotte d'une dizaine de terminaux identiques, jusqu'à des milliers de terminaux tous différents et tournant sous différents système d'exploitation (OS).

Respecter et faire respecter les recommandations de sécurité

Les principales fonctionnalités d'un MDM :

- Backup/Restore: Les comptes utilisateurs sont enregistrés sur le serveur de l'entreprise, permettant ainsi de les restaurer en cas de perte/renouvellement de mobile.
- Blocage et effacement à distance (dans le cas d'un vol de téléphone)
- Software Installation (Over The Air : OTA). Performance & Diagnostics: information sur la "vie" de votre terminal, telles que la batterie, les informations réseaux…
- Gestion du Roaming : pour bloquer l'installation d'applications sur des terminaux se trouvant hors d'un territoire géographique donné.
- FOTA – Firmware Over The Air : permet de mettre à jour les téléphones à distance.
- Monitoring: permet de contrôler les erreurs d'un parc entier.
- Prise de contrôle à distance: pour dépanner les utilisateurs
- Gestion d'inventaire: inventaire des terminaux actifs toujours à jour, consultation des communications en temps réel...

Différents type de MDM

1. Ceux qui ne peuvent gérer qu'un seul OS (RIM avec BlackBerry Enterprise Service, ou encore Microsoft avec son System Center MDM 2008)
2. La seconde catégorie d'offres, gère les principaux OS mobiles, parmi lesquels iPhone iOS, Windows Mobile, Windows Phone ou encore PalmOS, Symbian et Android.

Respecter et faire respecter les recommandations de sécurité

5.1.2 Mobile Application Management (MAM)

Les applications MAM proposent une protection applicative qui permet :

- de séparer l'application du système d'exploitation en l'isolant dans un bac à sable (sandbox),
- d'apposer des restrictions à l'usage du terminal (écriture, modification, diffusion, etc…).

5.1.3 Mobile Information Management (MIM)

Les applications MIM proposent une protection des informations sensibles

5.2 Aspect juridique

Que dit le Code du travail ?

L'entreprise a l'obligation d'assurer la sécurité des données car elle est responsable en cas de perte d'information. Quant à l'employé il doit respecter les règles de bonne conduite édictées par l'entreprise.

Ce principe simple n'est pas toujours évident à mettre en place car aucun texte de loi ne prend en compte la notion de données professionnelles sur un équipement personnel.

En effet, dans le cas de terminaux fournis par l'entreprise se pose la question de la vie privée résiduelle, c'est la cadre juridique qui délimite l'usage du matériel professionnel pour des raisons personnelles

Dans le cas de terminaux personnels (BYOD) se posent également plusieurs questions :

- Si l'entreprise efface le contenu d'un terminal mobile à distance, dont les informations privées du salarié, ce dernier peut-il porter plainte pour préjudice moral ou financier ?
- Si un employé détériore l'équipement d'un autre salarié, qui rembourse ?

Respecter et faire respecter les recommandations de sécurité

- Que se passe-t-il s'il faut enquêter sur le terminal mobile en cas d'incident ?

Que les terminaux mobiles soient fournis par l'entreprise ou qu'ils appartiennent aux employés, dans le carde du BYOD, il incombe donc à l'employeur de délivrer à ses salariés les bonnes informations d'usage et de les avertir des risques encourus

La **Charte Informatique** anticipe ainsi tout litige par l'encadrement de l'usage de l'équipement personnel au sein de l'entreprise.

La Charte Informatique doit définir :

- Les règles relatives à la sécurité du système d'information et à la confidentialité des données.
- Les règles posées quant aux sites et réseaux consultés
- Les règles de respect de la propriété intellectuelle
- Les modalités de contrôle et les sanctions possibles en cas de non-respect des dispositions de la charte.
- Le respect de la procédure afin de l'annexer au règlement intérieur de l'entreprise.