# LES REGLES ELEMENTAIRES DE SECURITE

# OBJETS NOMADES COMMUNICANTS

## CNRS – RSSIC – version 1.0 du 20 décembre 2012 – UTILISATEURS

Nous utilisons de plus en plus d'objets nomades communicants - téléphones intelligents, tablettes, etc. – pour accéder à des services via Internet.

Ces objets nomades doivent être considérés comme des ordinateurs à part entière. Par conséquent leur usage en milieu professionnel ne doit pas remettre en cause, et affaiblir, les politiques de sécurité en vigueur dans les établissements. Les personnels souhaitant faire l'acquisition de tels matériels doivent préalablement prendre conseil auprès de leur service informatique.

Les données manipulées sur ce type d'objets sont, la plupart du temps, des données personnelles mais également des données professionnelles sensibles (par exemple courrier électronique).

Le directeur d'unité est responsable de la sécurité des systèmes d'information de son unité, il a la responsabilité de faire connaitre et de faire appliquer les règlements de sécurité (politiques de sécurité, chartes, règles) promulgués par les tutelles dont il dépend.

**Il est essentiel que les *règles élémentaires de sécurité pour les objets nomades communicants* soient connues et mises en œuvre par l'équipe informatique et les utilisateurs, elles reposent sur :**

- La connaissance des précautions à prendre pour limiter les possibilités de vol ou de perte
- La protection des données contre le vol ou la perte
- La protection contre les codes malveillants
- La protection contre la fuite de données sur le réseau

L'engagement de l'utilisateur à respecter ces règles élémentaires de sécurité est une des conditions requises pour lui donner accès aux systèmes d'information – messagerie, agenda, etc. - hébergés sur le réseau local de l'unité. Cet engagement concerne tout objet nomade communicant autorisé à accéder au réseau local de l'unité, même si il appartient à l'utilisateur.

**Ces *règles élémentaires de sécurité pour les objets nomades communicants à l'attention des utilisateurs* sont détaillées dans ce document.**

*Le document « Règles élémentaires de sécurité pour les objets nomades communicants – ASR» est disponible sur le site SSI du CNRS, il détaille, à l'attention des équipes informatiques, les différentes possibilités de mise en œuvre en fonction des outils employés.*

*contacter votre informaticien ou celui de la DR / de l'université

## REGLES

1. **La connaissance des précautions à prendre pour limiter les possibilités de vol ou de perte**

   Les objets nomades communicants peuvent être facilement perdus ou volés, les vols surviennent souvent dans les transports mais également au bureau.

   - **Au bureau**
     - **Ne laissez pas votre SmartPhone ou Tablette en vue**
     - Fermez à clé la porte de votre bureau
   - **Dans les transports**
     - **N'oubliez pas votre matériel** … nombre de disparitions résultent d'un simple oubli
     - Ne laissez pas votre matériel en vue (dans une voiture, dans un train, etc.)
     - Ne laissez pas votre matériel sans surveillance (en particulier dans les trains)
     - Mettez un signe distinctif sur l'appareil et sa housse pour le surveiller plus facilement et évitez les échanges volontaires ou involontaires (à l'aéroport par exemple)
     - Utilisez éventuellement une dragonne
   - **Lors de déplacements à l'étranger**
     - **Prenez en compte les conseils** suivants : http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf
     - Faites attention lors des contrôles de sécurité dans les aéroports, contrairement à ce que l'on pourrait penser ce n'est pas un lieu sûr en ce qui concerne le vol d'objets
   - **Dans tous les lieux publics**
     - **Evitez d'utiliser votre matériel** sans s'assurer de ne pas être observé. Il peut tenter des voleurs opportunistes. En particulier masquez la frappe du code ou mot de passe qui permet de déverrouiller l'appareil.

2. **La protection des données contre le vol ou la perte***

   **Avant tout, il faut s'interdire de manipuler des informations sensibles via un service en ligne dont le fournisseur n'est pas le CNRS ou un de ses partenaires institutionnels (on n'a aucune maîtrise ni garantie de confidentialité sur les informations stockées dans un cloud public de type iCloud, SkyDrive, Google Drive, Gmail, Office 365, Google Apps, Amazon Elastic Compute Cloud , etc.).**

   Le paramétrage du terminal mobile permet de limiter les possibilités de vol de données lorsque celui-ci est entre les mains d'une personne malveillante :

   - **Verrouillage et chiffrement terminal mobile**:
     - **Configurez votre terminal pour qu'il se verrouille après 5 minutes d'inactivité avec activation par un mot de passe** (cela évite qu'en cas de perte ou de vol, l'appareil puisse être utilisé immédiatement)
     - **Activez l'effacement automatique** après un certain nombre de tentatives infructueuses pour entrer le mot de passe (l'attaquant devra utiliser des techniques élaborées avec accès direct au matériel pour passer outre)
     - **Utilisez un mot de passe dont la robustesse est fonction de la sensibilité des données que vous manipulez**. Les mots de passe dont la taille est inférieure à 5 chiffres sous iPhone et 6 caractères alphanumériques sous Androïd peuvent être

*contacter votre informaticien ou celui de la DR / de l'université

cassés par les pirates en moins d'une heure … Pour la sécurisation de données sensibles il est recommandé d'utiliser un mot de passe sur 8 chiffres sur un iPhone, 8 caractères au minimum sous Androïd.

- **Protégez votre mot de passe**, évitez d'utiliser votre matériel dans un lieu public sans vous assurer que vous n'êtes pas observé. En particulier masquez la frappe du code ou du mot de passe qui permet de déverrouiller l'appareil. Il ne faut jamais consulter, stocker, traiter sur un objet nomade des informations de sensibilité élevée dans un lieu public sans s'assurer que l'on n'est pas observé.
- **Activez le chiffrement des données** : configurez votre matériel pour chiffrer la mémoire permanente incluse dans l'appareil ainsi que les éventuelles mémoires additionnelles.

- **Blocage et effacement à distance en cas de vol**

  - **Lorsque cela est possible, activez la possibilité d'effacement à distance des données de votre terminal mobile**. Mais attention, n'utilisez que les procédures et outils maîtrisés et fournis par votre support informatique. *Les outils fournis par les opérateurs et/ou les éditeurs ou d'autres tierces parties – Icloud, GoogleApps, etc. – ne sont pas sûrs, ils vous géo-localisent, stockent d'autres informations personnelles qui vous concernent et certains de ces outils peuvent même récupérer toutes les informations que vous traitez sur votre terminal).* Cette protection sera de peu de secours face à un attaquant un tant soit peu déterminé qui souhaite récupérer vos données, il ne se connectera pas à un réseau Wifi, il ôtera la carte SIM.

    > ***La « messagerie unifiée » fournie par la DSI du CNRS permet de commander l'effacement à distance de façon native (*).*** *Cette commande est traitée lorsque le client se connecte au serveur. Ainsi, tant que l'objet n'a pas été mis en réseau et qu'une connexion à la messagerie n'a pas été effectuée, tous les messages stockés dans le cache de l'appareil restent disponibles et accessibles au voleur. Ainsi, si vos données sont très sensibles il convient d'inactiver ce cache ou de le limiter au minimum.*

  - **Notez les identifiants qui permettront le blocage des communications 3G de votre terminal mobile et conservez-les séparément**. Pour les Smartphones et Tablettes 3G, noter le numéro de téléphone, N° de la carte SIM et N° de code IMEI (*International Mobile Equipment Identity), c'*est un numéro unique attribué à chaque mobile qui est composé de 15 à 17 chiffres. *L'opérateur peut identifier un appareil qui tente de se connecter à son réseau et l'autoriser ou non. Le code IMEI sert en cas de vol à bloquer l'usage du mobile et aucune autre SIM ne pourra être insérée. Il sert aussi lors de la procédure du déblocage de votre mobile.*

- **Effacement des données avant un échange de matériel**. Avant un échange de matériel – changement de poste, utilisation d'un nouveau modèle, etc. – il convient de réaliser une remise à zéro complète du matériel pour le faire revenir à son état de sortie d'usine, éventuellement reformater le disque, etc.

- **Sauvegarde des données**. C'est le seul moyen de récupérer toutes les informations en cas de panne, perte ou vol, mais aussi avant un échange de matériel. Si l'utilisation est limitée à la messagerie et agenda en théorie les **données** sont stockées sur le serveur (*). Effectuez des sauvegardes en environnement sûr (poste de travail maîtrisé) et chiffrez ces sauvegardes.

*contacter votre informaticien ou celui de la DR / de l'université

**3. Protection contre les codes malveillants ***

Au quotidien des dizaines de failles sont découvertes dans les systèmes (Windows, iOS, Androïd) et logiciels (applications présentes et téléchargées depuis les plates-formes « stores » des éditeurs) qui équipent l'objet nomade communicant, ces failles sont très rapidement exploitées par des virus ou par des kits que mettent en ligne les pirates les plus expérimentés :

- **Ne cassez pas la protection du constructeur (jailbreaking)**. Cette pratique introduit de nouvelles vulnérabilités (plus aucun contrôle sur l'origine des applications téléchargées, portes dérobées installées avec l'outil de jailbreak, possibilité de récupération des informations stockées sans avoir à connaître le mot de passe).
- **Effectuez les mises à jour.** Effectuez les mises à jour avec les correctifs de sécurité fournis par le constructeur / éditeur. Il s'agit de se protéger des failles connues. Il faut noter que selon les plateformes, les vendeurs de matériels, les opérateurs téléphoniques ces mises à jour sont plus ou moins faciles voire impossibles à effectuer.
- **Limitez le chargement d'applications et limitez leur permissions** : il est possible de charger des applications fournies sur la plate-forme - « store » - de l'éditeur, mais il faut être vigilant vis-à-vis des applications que l'on installe. Il convient de vérifier leur réputation et ne les télécharger qu'à partir de boutiques officielles. Lors de l'installation n'accorder que les permissions nécessaires. Les applications malfaisantes constituent aujourd'hui la principale menace. Si des données très sensibles sont manipulées, il convient de s'interdire toute installation de logiciels non validés par le service informatique.