Vol de smartphone : assurer la scurit de sa vie numrique ?

Mobilit

Post par : JulieM

Publie le : 21/1/2016 14:30:00

En pleine sance de shopping, au restaurant, dans le bus, en vacances, ou lors d'une soire, les occasions ne manquent pas de se faire drober son Smartphone !

D'aprs une rcente tude mene par Lookout et IDG Research, 44% des Smartphones ont t vols parce que leurs propritaires les ont oublis dans un lieu public et 11% ont t vols l'arrache alors que le Smartphone tait dans la main de son propritaire, rang dans une poche, un sac main ou encore des bagages.

Les donnes ont plus de valeurs que le Smartphone.

Selon la mme tude, la moiti des victimes d'un vol de Smartphone seraient prts payer 500 \$ pour rcuprer leur tlphone, et plus d'un tiers des victimes dbourseraient jusqu' 1000 \$. Cette somme peut paratre surprenante, puisqu'elle permettrait de s'acheter un nouveau tlphone, mais elle est en ralit assez logique lorsqu'on pense toutes les donnes stockes perdues.

Le Smartphone contient des donnes prcieuses de notre vie numrique courriers lectroniques, contacts, photos, vidos, textos autrement dit, des informations personnelles et professionnelles importantes.

Les possibles consquences d'un vol de Smartphone peuvent tre dsastreuses :

- Perte des informations personnelles, et possible usurpation d'identit
- Utilisation frauduleuse de carte de crdit
- Perte des informations confidentielles de la socit, voire utilisation des fins frauduleuses
- Utilisation par les hackers du rpertoire de contacts pour diffuser des virus

3 tapes simples suivre pour assurer la scurit de votre vie numrique

Il existe des solutions spcifiques pour protger sa vie numrique. Cela commence avant mme l'utilisation du Smartphone. Les conseils suivants permettent de protger ses donnes et sa vie numrique du vol ou d'une utilisation criminelle :

1. Protection systmatique du Smartphone avec un mot de passe

Ne pas protger son tlphone avec un mot de passe est irresponsable, surtout lorsqu'il contient des informations professionnelles. Sans ce dernier, n'importe qui accde immdiatement la vie numrique de sa victime. Le mot de passe doit tre long (6 caractres de prfrence), avec des chiffres, des lettres, mais aussi des symboles. Il doit en outre tre utilis uniquement pour le Smartphone. Il est galement important de vrifier que le Smartphone se verrouille automatiquement ds qu'il n'est pas utilis.

La scurisation va connatre une nouvelle tape avec l'apparition et la dmocratisation - de tlphones disposant d'un systme d'identification par empreintes digitales.

2. Utilisation d'une application de géolocalisation pour Smartphone

En cas de perte ou de vol du Smartphone, de nombreuses applications permettent de le suivre à distance, de verrouiller et d'effacer le contenu du téléphone avant qu'un criminel ne puisse accéder et utiliser des données sensibles ou personnelles. Toutefois, certaines applications ne fonctionnent que si elles sont installées au préalable sur le téléphone.

Les constructeurs comme Apple, Samsung et Microsoft offrent des applications de localisation de Smartphones. L'utilisation d'applications mises au point par des tiers est également envisageable, mais la prudence doit être de mise, il faut bien vérifier la crédibilité de la source.

3. Utilisation d'une solution de sauvegarde de votre Smartphone

Les deux étapes précédentes peuvent décourager une utilisation criminelle des données, mais seule cette étape à savoir la sauvegarde des données mobiles permet de restaurer tout le contenu du téléphone. Une solution de sauvegarde de Smartphone permet de sauvegarder les photos, vidéos, contacts, événements, rappels et messages et restaurer les données sur un nouvel appareil.

Lors de la première sauvegarde de votre Smartphone, toutes vos données sont enregistrées dans le Cloud. Après cette première sauvegarde, seules les données qui ont été modifiées ou ajoutées seront automatiquement sauvegardées. Toutes les sauvegardes s'effectuent en arrière-plan pour ne pas empêcher l'utilisation parallèle du Smartphone.

Un Smartphone volé n'est presque jamais récupéré, il est cependant possible de limiter les risques d'utilisation frauduleuse des données et de récupérer tous les contenus de l'appareil et retrouver sa vie numérique rapidement et facilement grâce à une solution de sauvegarde dans le Cloud, commente Gaidar Magdanurov, General Manager Consumer Business chez Acronis