BSCI
Bertrand SCHMERBER
Conseil en Informatique
http://bertrandinformatique.free.fr

Conseil pour verrouiller son smartphone

Quelle méthode de verrouillage protège le mieux votre smartphone ?

Les systèmes d'exploitation modernes empêchent les intrus de deviner votre code d'accès (PIN ou mot de passe) en limitant le nombre de tentatives et en augmentant l'intervalle entre chaque nouvelle tentative. Mais est ce suffisant pour être protégé ?

- **Code PIN**

  Un code PIN (surtout un code long de six ou huit chiffres vraiment aléatoire) pourrait être une option sûre pour protéger votre smartphone. Mais, tout le monde a tendance à choisir un code facile à retenir (basé sur la date de naissance) et donc facile a deviner...

  Pour que le code PIN protège votre téléphone efficacement, il doit rester secret, mais vous déverrouillez votre smartphone presque une centaine de fois par jour. Dès lors, si quelqu'un cherche à découvrir votre code PIN, les occasions ne manquent pas.

- **Mot de passe**

  Un mot de passe complexe, avec des chiffres et des lettres, est beaucoup plus sûr qu'un code PIN de la même longueur. Il est plus difficile à deviner ou de le découvrir en cachette et de le mémoriser.

  Mais cette solution a un handicap ! Saisir un long mot de passe une centaine de fois par jour devient vite fastidieux. Une telle mesure de sécurité ne convient donc qu'en tant qu'option de secours, pour compléter une méthode plus pratique de déverrouillage de votre téléphone

- **Schéma de verrouillage**

  Le verrouillage par schéma est probablement le moyen le moins sécurisé ! En théorie, il existe presque 400 000 schémas possibles et certains sont vraiment complexes. Mais, dans la pratique, les gens utilisent des schémas courts et faciles à retenir.

  Par exemple, dans 50 % des cas, les schémas commencent dans le coin supérieur gauche, très prévisible ! Et bien sûr, les utilisateurs ont tendance à utiliser des formes simples (comme le Z de Zorro). Il est donc plus facile de deviner un schéma qu'il n'y paraît, surtout lorsqu'il est possible de jeter un coup d'œil par-dessus votre épaule ou en examinant les traces sur l'écran.

- Empreinte digitale

  Cette technologie est la plus sure, elle est apparue il y a plus de 10 ans et a donc fait ses preuves.

Bien sûr, cette solution n'est pas parfaite : il existe des façons d'accéder au téléphone en créant une fausse empreinte digitale, et des chercheurs ont démontré récemment qu'il est possible de procéder à une attaque par force brute sur le mécanisme de reconnaissance des empreintes digitales pour le déverrouiller

Cependant, il s'agit de techniques très sophistiquées qui nécessitent un niveau d'expertise élevé, du matériel sophistiqué et la motivation de consacrer beaucoup de temps et d'efforts au piratage. Par conséquent, pour la grande majorité des pirates l'authentification par empreinte digitale reste inviolable.

- Reconnaissance faciale

Il s'agit d'une méthode qui est assez facile à tromper. Parce que la très grande majorité des smartphones utilisent uniquement l'appareil photo frontal et pas vraie une reconnaissance en 3D

L'entreprise Google se prononce elle-même de manière assez claire à ce sujet. À ce jour, vous ne pouvez utiliser la reconnaissance faciale que pour déverrouiller l'écran, mais vous ne pouvez pas l'utiliser pour confirmer des paiements ni vous connecter à des applications !

Conclusion

En résumé, la combinaison de sécurité idéale pour les téléphones Android est l'utilisation de l'empreinte digitale pour le déverrouillage au quotidien, ainsi qu'un code PIN long (ou, mieux encore, un mot de passe fort) comme solution de secours.

Comme vous ne saisirez qu'occasionnellement votre code PIN ou votre mot de passe, vous pouvez vous permettre d'utiliser un plus grand nombre de caractères. Cependant, veillez à conserver votre mot de passe ou votre code PIN dans un endroit sûr au cas où vous l'oublierez.

N'oubliez pas de configurez votre écran de manière à ce qu'il se verrouille automatiquement après une période d'inactivité relativement courte.

Protégez aussi toutes les applications qui le nécessitent à l'aide d'un code PIN ou un mot de passe distinct, et si c'est possible par la reconnaissance de votre empreinte digitale pour en faciliter l'usage.

Si votre téléphone contient des informations hautement confidentielles

Une solution pratique est de stocker les informations vraiment confidentielles dans des dossiers cryptés

Certains smartphones Android (comme les Samsung) permettent d'activer la réinitialisation de l'appareil après un certain nombre de tentatives échouées de connexion, vous pouvez éventuellement envisagez cette option.

Pour avoir la sécurité la plus haute, utilisez uniquement un mot de passe long le moins souvent et le plus secrètement possible afin que personne n'ait la possibilité de le voir, mais là on frise la paranoïa.