20 façons de bloquer les attaques sur les mobiles

Wifi

• **N'autorisez pas votre appareil à rejoindre automatiquement des réseaux inconnus**.

• Désactivez toujours le Wi-Fi lorsque vous ne l'utilisez pas ou n'en avez pas besoin.

• **N'envoyez jamais d'informations sensibles via Wi-Fi à moins d'être absolument certain qu'il s'agit d'un réseau sécurisé**.

Applications

• N'utilisez que des applications disponibles dans la boutique officielle de votre appareil ; **ne téléchargez JAMAIS à partir d'un navigateur**.

• Méfiez-vous des applications de développeurs inconnus ou de celles dont les critiques sont limitées/mauvaises.

• **Tenez-les à jour** pour vous assurer qu'ils disposent de la sécurité la plus récente.

• S'ils ne sont plus pris en charge par votre boutique, supprimez-les !

• N'accordez pas de privilèges d'administrateur ou excessifs aux applications à moins que vous ne leur fassiez vraiment confiance.

Navigateur

• Méfiez-vous des publicités, des cadeaux et des concours qui semblent trop beaux pour être vrais. Souvent, ceux-ci mènent à des sites de phishing qui semblent légitimes.

• Portez une attention particulière aux URL. Celles-ci sont plus difficiles à vérifier sur les écrans mobiles, mais cela en vaut la peine.

• N'enregistrez jamais vos informations de connexion lorsque vous utilisez un navigateur Web.

Bluetooth

• **Désactivez l'appairage Bluetooth automatique**.

• **Éteignez-le toujours lorsque vous n'en avez pas besoin**.

Smishing (hameçonnage par SMS)

• Ne faites pas confiance aux messages qui tentent de vous amener à révéler des informations personnelles

• Méfiez-vous des tactiques similaires sur des plateformes telles que What's App, Facebook Messenger Instagram, etc.

• **Traitez les messages de la même manière que vous traiteriez les e-mails, réfléchissez toujours avant de cliquer !**

Vishing (hameçonnage vocal)

• **Ne répondez pas aux demandes d'informations financières personnelles par téléphone ou par e-mail**. Si vous êtes inquiet, appelez directement l'institution financière en utilisant le numéro de téléphone qui apparaît au verso de votre carte de crédit ou sur votre relevé mensuel.

• **Ne cliquez jamais sur un lien dans un e-mail commercial non sollicité.**

• Parlez uniquement avec des personnes en direct lorsque vous fournissez des informations sur le compte, et **uniquement lorsque vous lancez l'appel.**

• **Installez un logiciel qui peut vous dire si vous êtes sur un site Web sécurisé ou faux.**

Autres conseils utiles

Comme dans votre ordinateur, votre mobile contient beaucoup de vos données personnelles et il faut les protéger.

Personnalisez votre code pin, et activez le verrouillage automatique.

Il s'agit de la première protection face à une utilisation non autorisée de son mobile par un tiers. **Ne laissez pas le code PIN défini par défaut et évitez les codes faciles tels que 0000 ou 1234.**

Code à 6 chiffres, mot de passe, ou empreinte digitale : verrouillez votre mobile !

Il s'agit d'une précaution de base afin d'éviter qu'une personne tierce l'utilise sans votre autorisation. **L'utilisation d'un schéma peut sembler pratique mais cela reste moins efficace** que le mot de passe, le code à 6 chiffre ou l'empreinte digitale.

Créez et utilisez des mots de passe complexes et différents.

Nous créons des comptes en ligne régulièrement, et certains parmi nous continuent à choisir des mots de passe simples ou encore à utiliser toujours le même mot de passe. Il est prouvé que plus le mot de passe est complexe plus il difficile de l'usurper.

Un mot de passe est véritablement complexe lorsque celui-ci comporte un mélange de lettre (majuscules et minuscules), de chiffres et de symboles spéciaux de plus de 10 caractères.

Il existe également de nombreuses solutions en ligne pour gérer et conserver les mots de passe en sécurité, solution recommandée **https://keepass.fr/** Ce petit logiciel **libre, gratuit et en français, certifié par l'ANSSI (Agence nationale de la sécurité des systèmes d'information)**, permet de stocker en sécurité vos mots de passe pour les utiliser dans vos applications. KeePass dispose aussi d'une fonction permettant de générer des mots de passe complexes aléatoires.

Maintenez votre mobile à jour.

Au-delà des améliorations d'utilisation que peuvent apporter les mises à jour, il faut savoir que celles-ci comportent également souvent des modifications visant à renforcer la sécurité. **Il est donc important de maintenir votre mobile ainsi que vos applications à jour.**

Téléchargez les applications uniquement sur des plateformes légales.

Au moins 1/3 des fraudes en général vient de fausses applications téléchargées sur des sites malveillants. Privilégiez Google Play et/ou Apple Store pour télécharger vos applications.

Protégez-vous du phishing.

Que ce soit par email, sur les réseaux sociaux ou par SMS nous recevons beaucoup de messages nous incitant à cliquer sur un lien, télécharger ou ouvrir un fichier. Il faut rester toujours vigilant et ne pas donner suite à des messages suspects.

Autre point d'attention, certains fraudeurs peuvent essayer de vous duper afin de vous convaincre de leur transférer un code ou mot de passe à usage unique.

Il vous est alors vivement conseillé de ne pas donner suite à ce genre de sollicitation et ne jamais transférer à un tiers un code ou mot de passe à usage unique reçus par SMS. Et si vous souhaitez aider à lutter contre le phishing, rendez-vous sur les plateformes de signalement dédiées. **Par exemple, pour signaler les spams SMS, transférez par SMS le message reçu au numéro court 33700**. **https://www.33700.fr/**