Les solutions de paiement mobile et les systèmes de paiement sans contact

Les paiements via smartphone ou carte sans contact connaissent un engouement croissant. Payer ses courses sans argent liquide ni besoin de taper son code est certes confortable, mais recèle aussi des dangers.

Voici comment utiliser les moyens de paiement dématérialisés (sans contact) en toute sécurité :

- Protégez votre appareil mobile en verrouillant votre écran contre tout accès non autorisé et maintenez-le parfaitement à jour.
- Contrôlez les cartes bancaires, cartes de crédit ou prépayées, ainsi que les comptes de paiement mobiles que vous utilisez effectivement pour vos paiements sans contact. Si vous ne l'utilisez pas, faites en sorte de désactiver la fonction sans contact et annulez ou fermez les comptes de paiement qui ne vous servent pas.
- Fixez le plafond de vos dépenses et le montant limite de la transaction sans contact pour votre carte ou votre compte de paiement mobile – et donc le risque maximum – selon vos exigences.
- Ne versez sur vos cartes prépayées et comptes de paiement que les sommes d'argent dont vous aurez effectivement besoin dans un avenir proche.
- Sur l'application de paiement mobile, ne révélez que les données vraiment nécessaires et limitez au minimum les autorisations de l'appli.
- Vérifiez vos factures et signalez immédiatement à votre prestataire les paiements qui ne peuvent vous être attribués ou que vous n'avez pas effectués.
- Prévenez immédiatement votre fournisseur en cas de vol ou de perte de votre carte ou de votre dispositif mobile.

De la carte porte-monnaie à l'appli sur votre dispositif mobile

Les cartes bancaires offrent depuis longtemps aux consommateurs la possibilité de payer leurs achats, jusqu'à hauteur d'un certain montant, sans avoir besoin de taper leur code personnel. Des modes de paiement électroniques tels que Apple Pay ou Twint se sont ajoutés il y a quelques années et permettent d'effectuer des paiements sans contact à l'aide d'un smartphone ou d'une smartwatch (ce que l'on appelle « Mobile Payment »).

Avec la crise du coronavirus, ces procédés sont maintenant bien ancrés dans la vie quotidienne des consommateurs. Les avantages des dispositifs mobiles comme les smartphones et les tablettes sont évidents : pratiques, ils sont presque toujours à portée de main et connectés en permanence à Internet.

Par ailleurs, les systèmes de paiement mobiles seront bientôt incontournables : dès lors que l'on souhaite installer une appli payante sur son appareil mobile, il faut commencer par enregistrer les données de la carte de crédit avant de pouvoir régler ses achats en ligne « en mobilité » sans passer physiquement par la carte de paiement. Les solutions de paiement mobiles telles que Apple Pay, Google Pay ou Samsumg Pay fonctionnent pratiquement sur le

même principe, à la différence près qu'elles sont de plus en plus utilisées pour des achats off line, comme par exemple au supermarché ou à la station-service. La version suisse Twint fonctionne de façon similaire, même si elle n'est pas forcément liée à une carte de crédit, mais plus généralement à un compte bancaire ou à un crédit prépayé.

Les dangers des systèmes mobiles et sans contact

Bien que faciles et pratiques, les solutions de paiement sans contact comportent des risques liés à l'utilisation d'appareils mobiles et de cartes sans contact. De plus, l'absence d'éléments de sécurité tels que le code personnel ou le mot de passe facilite leur utilisation abusive.

Parmi les principaux risques, citons :

- la perte ou le vol de l'objet physique : si votre carte de paiement ou votre dispositif mobile tombent entre les mains d'une personne malveillante, celle-ci pourra en abuser pour effectuer ses propres achats. Selon le moyen de paiement et le plafond défini, l'addition peut vite grimper.
- le vol d'identité (https://www.ebas.ch/fr/vol-didentite/) : l'arnaque est possible même si la carte ou le dispositif restent toujours en votre possession. À travers des moyens pernicieux, tels que la diffusion de malwares (https://www.ebas.ch/fr/les-infections-par-malware/) , messages de phishing (https://www.ebas.ch/fr/le-phishing/) ou autres procédés d'ingénierie sociale (https://www.ebas.ch/fr/lingenierie-sociale-social-engineering/) , un escroc peut réussir à dérober par voie numérique vos identifiants de connexion ou vos informations de paiement, dans le but de réaliser des achats ou de faire des virements en votre nom.
- la violation de la vie privée : le propriétaire de l'appli n'a pas à savoir ce que le client achète ni où il effectue ses achats. De même, le commerçant ne doit pas connaître le solde disponible sur le compte de son client. Mais comment être sûr que ces règles sont effectivement respectées ? C'est donc à vous qu'il revient de décider quelles informations peuvent être utilisées, comment et par qui.

La bonne nouvelle, c'est que vous pouvez éviter efficacement tous ces tracas en suivant les recommandations que nous vous avons données plus haut.

Pour en savoir plus, consultez notre brochure « Mobile Banking et Mobile Payment» (https://www.ebas.ch/wp-content/uploads/2019/10/mobilebankingSKP_fr.pdf) ainsi que notre article intitulé Mobile Banking (https://www.ebas.ch/fr/les-applications-de-banque-mobile-mobile-banking/) .

Le paiement mobile est une solution de paiement dématérialisé sans contact réalisé au moyen de dispositifs mobiles tels que smartphones, smartwatchs et tablettes. Les cartes de débit et de crédit offrent également une fonction sans contact et sont de plus en plus liées à une application porte-monnaie. Le confort apporté par ces solutions doit être accompagné de quelques précautions pour garantir la sécurité de vos données et de votre argent.