

**Communiqué de presse**  
Zurich, le 25 novembre 2021

## **Acheter en toute sécurité avec la carte de crédit pendant la période précédant Noël**

**La carte de crédit est un des moyens de paiement les plus appréciés en Suisse – et aussi un des plus sûrs si on respecte les recommandations de sécurité les plus importantes. La Communauté suisse des prestataires de cartes bancaires (ISK) propose sur la plateforme «[lacartedecredit.ch](https://lacartedecredit.ch)» des recommandations utiles et actuelles sur le maniement en toute sécurité de la carte de crédit.**

La période précédant Noël est la période qui connaît les plus fortes ventes pour le commerce. C'est en conséquence aussi une période attractive pour les escrocs. Actuellement, les tentatives de phishing ou de smishing, avec lesquels on essaye de parvenir aux données de paiement à l'aide d'e-mails ou de SMS frauduleux, s'accumulent. La plateforme [lacartedecredit.ch](https://lacartedecredit.ch) informe comment les utilisateurs et le commerce peuvent se protéger contre les escroqueries.

### **Observer les mesures de sécurité simples**

Le capitaine Rolf Nägeli de la Police municipale de Zurich estime que le paiement avec la carte de crédit est très sûr si quelques règles peu nombreuses mais importantes sont respectées. Il le sait d'expérience: «La technologie est sûre. Le point faible est l'homme». L'officier de police expérimenté recommande d'observer des mesures de sécurité simples et que la plupart des utilisateurs de cartes connaissent bien. Elles ne sont ni compliquées ni nouvelles, mais vous devez continuer à vous en souvenir et, surtout, les suivre de manière cohérente. [Lien vidéo](#)

### **Actuellement: phishing et smishing**

Les tentatives de phishing et de smishing (ces derniers par SMS) sont actuellement le type d'escroquerie le plus fréquent sur Internet. Les escrocs essayent dans ce cadre à parvenir aux données de paiement à l'aide d'un e-mail ou d'un SMS semblant authentique à s'y méprendre et d'un lien dirigeant vers une page Internet falsifiée. Il est ici important de savoir: par principe, les émetteurs de cartes de crédit ou les banques ne demandent jamais par e-mail à leurs clients d'entrer ou de changer leurs données de paiement. Les demandes de paiement par e-mail doivent constamment être confirmées avec l'émetteur du paiement. [Lien](#)

### **Les pickpockets numériques ne sont pas à craindre**

Par opposition, les pickpockets numériques qui rodent avec un lecteur de carte et tentent,

à l'aide d'une fonction sans contact ou NFC (Near Field Communication), de tirer profit de cartes de crédit ou de débit, ne représentent aucun danger sérieux. Certes en théorie, ce serait possible. La pratique montre cependant que de tels vols numériques de pickpockets se produisent très rarement – l'effort à fournir est trop grand par rapport au rendement éventuel. [Lien](#)

#### **Qui est responsable si quelque chose se produit quand même?**

Il n'y a pas de sécurité à cent pour cent. Les utilisateurs de cartes de crédit ont toutefois la certitude que l'émetteur de carte prendra en charge le dommage après avoir vérifié les faits, pour autant que les obligations de diligence aient été respectées. La même chose vaut pour le commerce, où le risque de défaillance de paiement ainsi que les dépenses considérables que représentent la gestion des relances et de l'encaissement disparaissent grâce à la garantie de paiement. [Lien](#)

Vous trouverez de plus amples informations relatives au maniement en toute sécurité de la carte de crédit sur [lacartedecredit.ch](http://lacartedecredit.ch)

#### **Au sujet de l'ISK**

La Communauté suisse des prestataires de cartes bancaires (ISK) s'engage pour la promotion du paiement sans espèces, par carte de crédit.

Lien vers la page de campagne: [lacartedecredit.ch](http://lacartedecredit.ch)