Lettre Cyber 67

Novembre 2022

Les paiements par carte bancaire sur Internet :

Les achats sur le Web ont pris une place prépondérante dans notre vie quotidienne. La France compte plus de 200 000 sites marchands sur internet. L'approche des fêtes de fin d'année va sans nul doute relancer le commerce électronique. Si dans une grande majorité des cas, les opérations de paiement se passent sans soucis, il est nécessaire d'avoir quelques réflexes simples pour sécuriser vos paiements

1 / Attention aux réseaux Wi-Fi publics : Un réseaux Wi-Fi non sécurisé peut être facilement observé. Un pirate peut installer sur votre terminal un logiciel malveillant et intercepter vos données.

2 / Veillez au sigle de paiement sécurisé : Entrez uniquement vos coordonnées bancaires dans un formulaire comprenant une sécurisation HTTPS. En règle général il s'agit d'un petit cadenas visible dans la barre d'adresse de votre navigateur.

3 / Ne communiquez jamais vos informations bancaires : Ne communiquez jamais votre numéro de carte bancaire ainsi que le cryptogramme visuel (trigramme) par téléphone, par mail ou via un canal non sécurisé spécialement prévu à cet usage.

4 / Activez la double authentification : Mettez en place une double authentification de paiement proposée par les organismes bancaires. Elle peut se matérialiser par un code secret demandé juste après un paiement. Celui-ci peut vous être envoyé par SMS, par mail, par téléphone, le code SMS étant le plus souvent utilisé.

5 / Privilégiez la sécurité au gain de temps : Il est préférable de ne pas enregistrer votre carte sur une application smartphone. La CNIL recommande la non-conservation des données relatives à la carte de paiement sur l'application ou dans le navigateur des clients dans la mesure où ces terminaux ne sont pas nécessairement conçus pour garantir une sécurité optimale des données bancaires.

6 / Méfiez-vous des sites inconnus : Certains sites malveillants peuvent prendre l'apparence d'un site marchand ou de paiement que vous connaissez. **Avant d'acheter :** Renseignez-vous sur la réputation du site / Privilégiez les sites connus / Prenez connaissance des notes et avis des consommateurs / Méfiez-vous des offres alléchantes.

Recevoir cette lettre info par mail, envoyez-nous votre demande :
Arnaud.schweitzer@gendarmerie.interieur.gouv.fr ou mathieu.knobloch@gendarmerie.interieur.gouv.fr

6 / Bien entendu, il ne faut pas oublier aussi…. :

- Sécurisez votre terminal informatique : Mise à jour régulière des équipements, utilisation d'un anti-virus et d'un pare-feu, sécurisation des accès.
- Consultez régulièrement vos comptes bancaires en ligne afin de vérifier qu'aucune transaction douteuse n'a été réalisée.
- Sécurisez vos mots de passe : Variez- les, si possible attribuer un mot de passe pour chaque usage. Un mot de passe doit contenir au moins douze caractères (Majuscule, minuscule, chiffre et caractères spéciaux).
- Utilisez votre messagerie de façon sécurisée : Lisez attentivement les informations contenues dans les courriels, ne cliquez pas sur les pièces jointes ou les liens qui paraissent douteux….

6 / En cas d'incident…. :

Si vous constatez avoir été piraté suite à un achat en ligne, **contactez tout d'abord votre banque** pour faire opposition sur votre carte bancaire et pour ensuite demander le remboursement des opérations frauduleuses ou demander l'attribution d'une nouvelle carte bancaire.

Vous pouvez ensuite **signaler ce piratage sur Perceval**, la plateforme de signalement des fraudes à la carte bancaire.

Recevoir cette lettre info par mail, envoyez-nous votre demande :
Arnaud.schweitzer@gendarmerie.interieur.gouv.fr ou mathieu.knobloch@gendarmerie.interieur.gouv.fr