FRAUDE AUX PAIEMENTS EN LIGNE - LES DANGERS DE LA DIRECTIVE DSP2

Categories: Banques & organismes de crédit, Gestion compte (C.B, chèques, vol, frais bancaires), Les conseils
Tags: Actualités, Conseils

Nous publions une fiche de la DGCCRF sur les fraudes à la carte bancaire qui ont connues un augmentation considérable. Cet accroissement est lié principalement au contournement de la directive DSP2 entrée en vigueur en juillet 2021. Les escrocs interviennent avant toute opération !

Depuis la fin des années 2000, la sécurité des paiements en ligne s'est renforcée grâce aux déploiements de solutions d'authentification des transactions par carte. D'abord poussée par l'Observatoire de la Sécurité des Moyens de Paiement (OSMP), présidé par la Banque de France, les solutions d'authentification forte se sont généralisées depuis 2019 avec la 2e directive européenne sur les services de paiement (DSP2).

Bien que les résultats soient très positifs, l'authentification forte ne constitue pas un rempart absolu contre la fraude : de nouveaux types de fraude sont en effet apparus pour contourner l'authentification forte en manipulant le porteur de la carte...

Principes / Définitions :

L'authentification forte des achats en ligne

La 2e directive européenne sur les services de paiement (DSP2), entrée en application en 2019, dispose que les transactions par carte sur internet soient en principe soumises à une authentification forte du payeur. Celle-ci consiste à vérifier la légitimité de l'opération en vérifiant, par l'intermédiaire d'un protocole appelé 3-D Secure, deux éléments que seul le payeur peut mobiliser : il s'agit d'un élément de connaissance (mot de passe, code…), d'un élément de possession (téléphone, clé USB, carte…) et/ou d'un élément biométrique (empreinte digitale, biométrie faciale…). En pratique, les principales solutions d'authentification forte sont les suivantes :

- L'application mobile bancaire via lequel le client renseigne un code spécifique pour ses achats en ligne ou présente son empreinte biométrique ;
- **Ou** la réception d'un mot de passe à usage unique par SMS complété par un code spécifique pour les achats en ligne ;
- **Ou** l'utilisation d'un appareil physique mis à disposition par la banque (générateur de codes doté d'un clavier de saisie, clef USB ou lecteur de QR-Code)

Certaines transactions par carte sont toutefois éligibles à des exemptions, comme les transactions de faible montant (moins de 30 euros) ou avec un faible niveau de risque car conforme aux habitudes de paiement. Dans tous les cas, la banque du payeur reste en capacité de décider ou non de demander une authentification forte.

Le contournement de l'authentification forte

Les fraudeurs vont d'abord collecter des données sur leur cible et se renseigner sur elle. Par des attaques informatiques (phishing, malware, dark web), ils vont notamment récupérer les coordonnées bancaires et les données de sa carte bancaire (numéro, nom du titulaire, date d'expiration, code à 3 chiffres sur le dos de la carte).
Le fraudeur va ensuite utiliser ses données bancaires puis au même moment **contacter** sa victime, généralement par téléphone. Pour l'installer dans un environnement de confiance, le fraudeur va alors usurper l'identité de sa banque via la technique du spoofing, en disant être conseiller bancaire ou travailler dans le service anti-fraude. Il prétend alors devoir réaliser un test de sécurité ou vérifier certains éléments pour bloquer les tentatives de fraude en cours.
La victime est enfin invitée à **valider les opérations via ses moyens d'authentification forte**. Il peut s'agir d'un paiement par carte sur internet, d'une opération de virement, du rajout d'un bénéficiaire de confiance, d'une modification de plafond sur la carte, de l'enrôlement dans une solution de paiement mobile ou encore du transfert du moyen d'authentification forte.

Via ce type d'attaque, le fraudeur amène en fait sa victime à valider à son insu des opérations frauduleuses en passant outre les différentes alertées adressées par la banque.

Ressources vidéos pour comprendre les fraudes aux paiements en ligne :
• Vidéo de la Banque de France sur l'authentification forte :
Sécurité des paiements en ligne : qu'est-ce qui va changer ? | Banque de France - YouTube
MESSAGE DE PRÉVENTION :

1. **Ne répondez pas aux sollicitations des fraudeurs :** utilisez toujours un canal sécurisé et connu (favori, moteur de recherche) pour vous connecter à votre banque ou vos fournisseurs de services ; ne cliquez jamais sur un lien reçu par mail ou SMS
2. **Refusez toute communication non sollicitée** qui vous serait proposée en direct (téléphone, chat…) et recontactez votre banque par votre canal habituel : votre banque ne vous demandera jamais de valider à distance une opération à des fins de test ou en réponse à une fraude ; si elle suspecte une opération de fraude, votre banque est en capacité de la bloquer sans avoir à vous demander votre intervention
3. **Utilisez à bon escient vos outils et données d'authentification et protégez-les :** vos outils et données d'authentification sont aussi sensibles que le code de votre carte bancaire
4. **N'utilisez jamais vos outils et données d'authentification pour des opérations dont vous n'êtes pas à l'origine et ne les communiquez jamais à un tiers**

Je suis victime, que faire ?

Si vous recevez une demande d'authentification non sollicitée sur votre téléphone ?

- **N'y donnez suite que si vous êtes à l'origine de l'opération**
- Dans le cas contraire, contactez immédiatement votre banque car cela peut indiquer que vos coordonnées bancaires ont été piratées

Si vous êtes contacté par téléphone pour authentifier une transaction ?

- **Cessez immédiatement tout échange avec l'interlocuteur** et en cas de doute rappelez votre banque par votre canal habituel
- Ne donnez surtout pas suite aux invitations à valider les opérations

Et si vous avez déjà authentifié les opérations frauduleuses ?
Contactez immédiatement votre banque pour, selon les situations, mettre en opposition votre carte et/ou renouveler vos données et outils d'authentification.
Contestez les opérations en question auprès de votre banque, en suivant la procédure indiquée, de façon à étudier la possibilité d'un remboursement (article L133-18 et L133-19 du code monétaire et financier).
Attention, dans ces situations, le remboursement n'est pas de droit car l'authentification forte d'une opération peut constituer une négligence grave qui engagerait votre responsabilité dans les

opérations contestées. S'il appartient à la banque de justifier le refus de remboursement par des éléments en fait et en droit et d'apporter la preuve de la négligence grave, conservez toute pièce et élément relatif à ces opérations qui puisse attester de la sophistication de la manipulation dont vous avez été victime (SMS, copie-écran etc.)
Dans tous ces cas - Vous pouvez signaler auprès des forces de l'ordre et de façon confidentielle une fraude à la carte bancaire via le service PERCEVAL accessible via service-public.fr

Pour l'éviter, un truc simple ! Quelque soit l'appelant, ne donnez aucune information. Indiquez à votre interlocuteur que vous allez le rappeler. L'escroc ne travaille pas bien sur dans la vraie banque. Il est possible maintenant de masquer le numéro utilisé et d'afficher le numéro que l'on veut ! En rappelant le vrai numéro de votre banque, vous aurez la certitude de l'arnaque...

Notre association gère de nombreux dossiers liés à cette escroquerie.

Si votre banque ne veut pas vous annuler les opérations, contactez avec le lien ci-après
http://adcfrance.fr/contactez-nous/

Vous trouverez déjà des informations ci-dessous :

L'association fera le maximum pour vous aider. Il vous sera simplement demandé une adhésion à 47 € incluant l'abonnement à notre revue trimestrielle dont vous trouverez deux numéros dans les liens ci-dessous :

Les conseils pratiques pour la gestion d'un litige

Le numéro 152 de la revue Antipac

L'apparition de l'ADC France :

La revue Antipac n° 149

Vous pouvez la réaliser avec le lien sécurisé ci-dessous :

http://adcfrance.fr/adhesions-readhesions-adc-france/

Vous pouvez aussi nous l'adresser par chèque à l'ordre de l'ADC France 3/5 Rue Guerrier de Dumast, 54000 NANCY