

DANS TOUS LES CAS

En cas de difficultés avec votre banque, vous pouvez vous adresser à l'Association Française des Usagers des Banques (AFUB).



SOYEZ PRUDENT SUR INTERNET

Être prudent sur Internet, c'est d'abord ne pas avoir peur de tout. Pour détecter les pièges, il suffit souvent de se dire : « si un inconnu me disait ça dans la rue, est-ce que je le croirais ? ».

La prudence sur Internet, c'est aussi résister aux tentations du téléchargement illicite et se méfier du sentiment d'anonymat.

Une plateforme de signalement vous permet de signaler les contenus illicites de l'internet :

www.internet-signalement.gouv.fr



CVEC
Contribution
Vie Étudiante
et de Campus

PAYER VOTRE CVEC

Pour régler la CVEC, c'est sur cvec.etudiant.gouv.fr et nulle part ailleurs, soyez vigilant.e face aux sites frauduleux.



LA MISSION DU SERVICE SOCIAL EN FAVEUR DES ETUDIANT.E.S

Le service social inscrit son action dans le cadre de la mission générale du Crous : contribuer à l'amélioration des conditions de vie et de travail des étudiant.e.s.



L'INTERVENTION AUPRÈS DES ÉTUDIANT.E.S

Les assistantes sociales reçoivent l'ensemble des étudiant.e.s inscrite.e.s dans un établissement d'enseignement supérieur publics ou privé.



+ D'INFOS

www.crous-bordeaux.fr/social/



Mise en garde contre le piratage et les fraudes et les arnaques



ARNAQUES :

AU COMPTE BANCAIRE

À LA CARTE BANCAIRE

AU « CHÈQUE DE L'AMITIÉ »

AUX ANNONCES DE LOGEMENT

AU PIRATAGE DU TÉLÉPHONE

www.crous-bordeaux.fr





PIRATAGE DU COMPTE BANCAIRE

QUE FAIRE ?

Contactez rapidement votre conseiller pour l'informer et éviter des frais bancaires, puis lui envoyer une lettre recommandée pour contester le(s) débit(s), demander le remboursement par écrit, la banque doit le faire dans les 30 jours, et joignez la copie du dépôt de plainte ou main courante ;

Faire opposition à votre carte bancaire ;

Si l'opposition est tardive ou si vous avez été trop négligeant le remboursement peut être partiel ;

RECOMMANDATIONS

Vérifier vos comptes régulièrement (les débits même les petites sommes), changer régulièrement votre mot de passe « compliqué ». Utiliser le générateur de mot de passe complexe de la CNIL disponible sur www.cnil.fr ;

Lorsque vous faites un achat en ligne, vérifier que le site internet est sécurisé (il doit y avoir un cadenas vert à côté du «https» dans URL) ;

Sélectionner vos e-mails avant de les ouvrir, ne pas cliquer automatiquement sur tous les liens, ne pas avoir peur des messages alarmistes, vérifier les fautes d'orthographe ainsi que les mauvaises présentations dans les emails.

Vous doter d'un bon anti-virus.

À SAVOIR

Une banque ou autre organisme **ne vous demandera jamais** de divulguer votre identifiant et votre mot de passe dans un email ou par téléphone.



PIRATAGE PAR TÉLÉPHONE OU FRAUDE À LA CARTE SIM

C'est une technique de renvoi d'appel qui permet de passer outre le processus d'identification des banques par SMS : le « 3D sécurisé ». Votre ligne téléphonique n'est plus en service, votre répondeur est détourné vers un numéro inconnu.

QUE FAIRE ?

Appeler au plus vite le service client de votre opérateur qui va annuler le transfert d'appel (et reconfigurer votre box si nécessaire) et vous demander de changer votre mot de passe. Pensez à porter plainte.



LA FRAUDE DU « CHÈQUE DE L'AMITIÉ »

1. Un inconnu vous met en confiance puis a besoin que vous lui rendiez un service : il vous propose d'encaisser un chèque (souvent d'un montant important) que lui-même ne peut pas encaisser pour diverses raisons.

2. Il vous demande de retirer de votre compte la majeure partie de cette somme d'argent en espèces afin de lui donner, et vous laisse le reste de cette somme pour vous aider, ou vous dédommager comme une « commission ».

3. Le chèque que vous encaissez est enregistré sur votre compte en solde positif, mais **48h après vous recevez une alerte de votre banque indiquant que ce chèque est déclaré « impayé ».**

4. Vous êtes débiteur de la totalité de la somme, et il n'y a pas de recours possible.



LES ARNAQUES DES ANNONCES DE LOGEMENT

Vous êtes en recherche d'un appartement ou d'une colocation, certaines annonces peuvent être des pièges. Soyez vigilants vis-à-vis des demandes insolites qui doivent attirer votre attention :

- demande d'envoi d'argent pour la réservation ;
- photo sans relation avec le lieu ;
- loyer faible par rapport au marché ;
- loyer doublé d'une demande de service.

Vous envoyez un email au « propriétaire » et après quelques échanges d'emails, il vous demande d'envoyer de l'argent par Mandat Cash.

Vous ne devez jamais verser d'argent avant la signature du bail ! Cessez donc tout contact avec cet individu et signalez l'annonce via la plateforme de signalement (www.internet-signalement.gouv.fr)

Dans tous les cas :

- n'envoyer de l'argent liquide qu'à des personnes que vous connaissez ;
- ne jamais remettre d'argent avant d'avoir visité le logement ;
- régler par chèque ou virement bancaire ;
- n'envoyez pas de photocopies de vos papiers d'identité.

Vous cherchez un logement ? Pensez à la plateforme sécurisée www.lokaviz.fr, gérée par le Crous.

+ des offres de logements Crous toute l'année