



## Conseils de sécurité lors de l'utilisation d'Internet, des cartes bancaires et de l'e-banking.

Face à la recrudescence des actes de malveillance et des opérations frauduleuses liés à l'utilisation d'Internet, des cartes bancaires et de l'e-banking, la BCJ souhaite vous informer des risques connus à ce jour et des moyens pour vous prémunir contre les malfaiteurs. La liste des recommandations émises par la BCJ n'est pas exhaustive.

## Internet

### Utilisation d'Internet

L'utilisation d'Internet reste sûre à condition de respecter quelques règles élémentaires. Vous avez un rôle actif à jouer pour assurer la sécurité de votre ordinateur et des informations que vous échangez par Internet. La protection de votre ordinateur relève de votre responsabilité.

### Nos conseils de sécurité

- **Protégez votre ordinateur**

Installez un logiciel de sécurité Internet (antivirus, pare-feu, etc.).

N'installez que des programmes fiables (téléchargez ou achetez auprès de sites Internet, sociétés, magasins de confiance).

Maintenez à jour votre ordinateur, navigateur Internet et logiciel de sécurité Internet.

Sécurisez votre routeur avec un mot de passe.

- **N'utilisez que des sites sécurisés pour vos opérations financières ou confidentielles**

Contrôlez et vérifiez l'adresse des sites que vous consultez (les adresses des sites sécurisés commencent par https et il apparaît un cadenas à droite de la barre d'adresse).

Ne transmettez des informations personnelles ou confidentielles (par exemple votre adresse courriel) qu'à des sociétés connues et fiables.

- **Protégez vos moyens d'authentification**

Ne transmettez à personne vos codes d'accès, même à la banque.

Mémorez votre mot de passe et ne l'écrivez nulle part.

Refusez l'enregistrement des mots de passe sur votre ordinateur ou navigateur.

- **Adoptez un comportement prudent sur Internet**

Evitez de télécharger des fichiers sur Internet (forums publics, réseaux peer to peer, etc.). La plupart des virus sont transmis aujourd'hui par ce canal.

N'ouvrez pas de courriels d'expéditeurs inconnus et faites analyser, par votre logiciel de protection Internet, les courriels qui contiennent un fichier attaché.

Ne communiquez votre adresse courriel qu'à des tiers de confiance (comme votre banque).

Soyez vigilant avec les pseudo messages provenant de votre banque : certains pirates falsifient les adresses courriel et tentent de se faire passer pour votre banque.

N'utilisez pas des connexions WIFI (réseau sans fil) non ou mal sécurisées pour vos opérations bancaires.

## Phishing

Le phishing a pour but de vous rediriger à votre insu vers un site pirate, très semblable à celui d'origine, dans l'objectif de récupérer vos données confidentielles (numéro de compte, données relatives à la carte de crédit, etc.). Les malfaiteurs utilisent des mails, très semblables à ceux des banques, demandant des informations confidentielles.

### Comment se préserver ?

- Ne jamais ouvrir des mails de provenance inconnue.
- Ne jamais communiquer ses codes ou ses mots de passe sur Internet. La BCJ ne demande jamais d'informations confidentielles que ce soit par mail, téléphone, lettre.
- Lors de connexions sur un site sécurisé, assurez-vous que l'adresse du site commence bien par https et vérifiez l'apparition du cadenas à droite de la barre d'adresse. En cas de doute, déconnectez-vous immédiatement.
- Privilégiez la saisie de l'adresse Internet choisie au lieu de l'accès via un lien reçu par mail.

## Cartes bancaires

### Utilisation frauduleuse par des tiers

L'abus de carte est l'utilisation illégitime d'une carte par un tiers non autorisé. Les variantes d'abus de carte de paiement sont multiples : utilisation d'e-mails dit de phishing, skimming ou encore vol de carte. En cas de vol ou de perte de votre carte, présentez-vous au guichet de l'une de nos succursales ou agences ou contactez les numéros d'urgence que vous trouverez au verso de la brochure. Votre carte sera immédiatement bloquée et remplacée.

### Nos conseils de sécurité

- A la remise de votre carte, signez-la. Notez à part votre numéro de carte: il vous sera demandé pour toute opposition en cas de perte, de vol ou d'utilisation frauduleuse.
- Votre code NIP (numéro d'identification personnel) est confidentiel: ne le rangez jamais avec votre carte, ne le notez même pas, sous aucune forme que ce soit. Apprenez-le par cœur, ne le communiquez à personne, en aucune occasion.
- Ce code NIP vous permet d'effectuer des transactions aux distributeurs automatiques d'argent, dans les commerces, aux stations d'essence et aux caisses des parkings. Vous devez toujours maintenir ce code secret. Ne choisissez pas un code facile à reconstituer, comme une date de naissance, un numéro d'immatriculation, etc.
- Lors d'un retrait d'espèces au bancomat, assurez-vous que personne ne vous observe lorsque vous saisissez votre code NIP, et n'acceptez pas l'aide d'inconnus. Lorsque que vous tapez votre code, utilisez votre autre main pour le cacher.
- Vérifiez toujours que vous avez récupéré votre carte après un paiement ou un retrait d'espèces.
- Ne perdez jamais de vue votre carte de crédit (ex. dans un restaurant).
- Pour vos achats sur Internet, privilégier l'utilisation d'une carte à prépaiement. Vous chargez simplement votre carte avec le montant désiré. De plus, la carte PrePaid n'est pas liée à votre compte bancaire.
- Utilisez, avec la plus grande précaution, les données personnelles telles que le numéro de votre carte de crédit, sa date d'échéance, ou son code CVV/CVC<sup>1</sup>. Ne communiquez en aucun cas ces données par courrier électronique, à l'aide de formulaires Web non sécurisés ou ouvertement par la poste, même si l'on vous donne l'assurance que la carte ne sera pas débitée.

# Skimming

Le skimming est une opération frauduleuse qui consiste à intervenir sur un bancomat et à en modifier certains composants afin de récupérer des informations sur la bande magnétique. Le code PIN peut être récupéré par une caméra qui filme l'introduction du code. Les malfaiteurs peuvent, à l'aide de ces informations, fabriquer de fausses cartes qui leur permettent de débiter les comptes des clients piégés.

## Comment se préserver ?

- Vérifiez que le bancomat ne présente aucune anomalie. En cas de doute prenez contact avec la BCJ.
- Vérifiez également les lecteurs de cartes dans les commerces (station d'essence, gares, etc.)
- Entrez votre code à l'abri des regards indiscrets lorsque vous retirez de l'argent au bancomat.
- Placez une main au-dessus du clavier dans le but d'empêcher que celui-ci soit filmé.
- N'oubliez pas de reprendre votre carte et votre reçu.
- Ne vous laissez pas distraire lors de vos opérations au bancomat.
- Si votre carte reste bloquée, refusez l'aide d'une personne inconnue, ne recomposez surtout pas votre code et informez-nous.
- En dehors des heures d'ouverture, l'accès à un local disposant de bancomats (zone 24h) se fait uniquement en engageant la carte dans un lecteur. Le code NIP n'est jamais demandé.
- Demandez le blocage immédiat de votre carte si des anomalies sont constatées.

<sup>1</sup> Les codes CVV (Code Verification Value) et CVC (Card Verification Code) sont des codes de sécurité composés d'une suite de trois chiffres qui se trouvent au dos de votre carte de crédit et qui permettent de confirmer que vous êtes en possession de votre carte lors de transactions en ligne.

## E-banking

### Sécurité

La BCJ met à disposition un système fiable et sécurisé afin de vous permettre d'utiliser nos services en ligne. Afin de réduire les risques dans les cas de fraudes, la BCJ vous recommande de limiter le nombre de comptes pour lesquels vous souhaitez faire des transactions par internet et de préférer, le plus souvent possible, le mode de consultation et d'utiliser, pour les transactions, des comptes ayant des soldes peu importants.

### Nos conseils de sécurité

- Disposez d'un antivirus reconnu et d'un pare-feu (FireWall), assurez-vous qu'ils sont à jour et scannez fréquemment l'ordinateur.
- Passez toujours par le site <http://www.bcj.ch> pour aller sur le BCJ-Net.
- Vérifiez l'apparition du cadenas à droite de la barre d'adresse sur lequel vous pouvez cliquer (une identification du site s'ouvre et en prouve l'authenticité).
- Lors de votre connexion au BCJ-Net, assurez-vous que l'adresse du site commence bien par https. En cas de doute, déconnectez-vous immédiatement.
- Travaillez avec un seul navigateur ouvert et une seule page ouverte.
- Si une anomalie survient pendant la session (exemple: veuillez patienter pendant la mise à jour), fermez immédiatement la connexion et éventuellement contactez la BCJ.
- Déconnectez-vous correctement de la session (ne pas uniquement fermer son navigateur mais cliquer sur « Déconnexion »).

## Clé BCJ-Net

Pour sécuriser vos opérations bancaires en ligne, la BCJ vous propose la clé BCJ-Net. Ce système fonctionne avec une clé USB et une carte à puce intégrée. Il vous garantit une utilisation simple et une connexion hautement sécurisée pour vos opérations bancaires en ligne via le BCJ-Net. Pour toute commande de clé, merci de vous présenter au guichet de l'une de nos succursales ou agences ou de nous contacter.

### Les avantages de la clé BCJ-Net

- Sécurité accrue pour vos opérations en ligne
- Simplicité d'utilisation
- Utilisable sur tout PC ou Mac équipé d'un raccordement USB ouvert et d'une connexion Internet
- Aucun logiciel ou pilote à installer



## Numéros d'urgence.

### En cas de perte, vol ou blocage de carte.

#### Carte BCJ

+41 (0)32 465 13 01      Durant les heures d'ouverture de la banque  
+41 (0)44 271 22 30      En dehors des heures d'ouverture de la banque

#### Carte Maestro

+41 (0)32 465 13 01      Durant les heures d'ouverture de la banque  
+41 (0)44 271 22 30      En dehors des heures d'ouverture de la banque

#### Carte Visa / Mastercard

+41 (0)58 958 83 83      Perte de la carte 24h / 24 et service d'urgence

#### Carte TravelCash

+41 (0)31 710 12 15      Perte ou vol de la carte  
+41 (0)31 710 11 11      Service client Swiss Bankers (lun - ven de 8h à 17h)