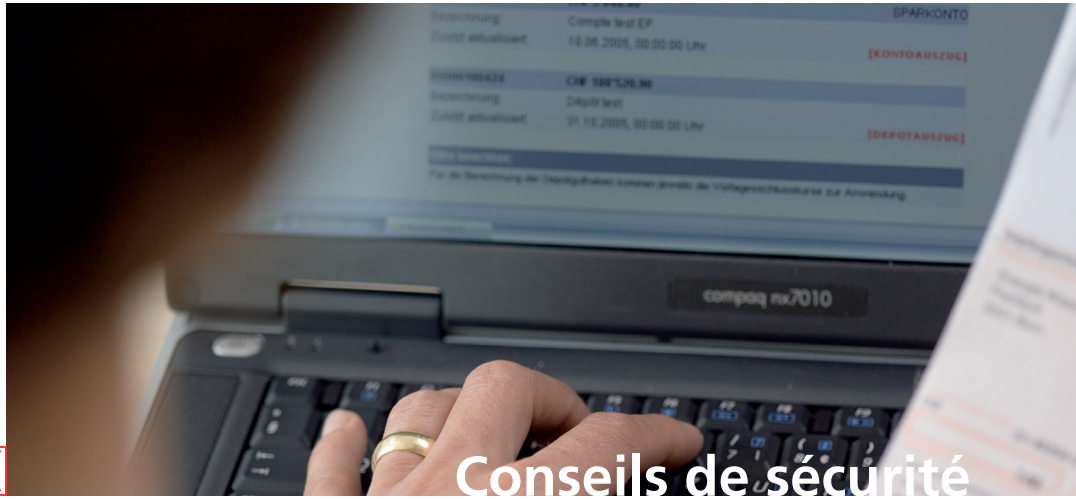

Conseils de sécurité

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

BCJ

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 (internet security y compris 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, le navigateur Internet et le logiciel de sécurité Internet.

  Sécurisez votre routeur avec un mot de passe différent du mot de passe par défaut.

- **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.

  Mémorisez 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, malware, chevaux de Troie, 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.

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 ou des sites publicitaires, 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 ou sur notre site www.bcj.ch. Votre carte sera immédiatement bloquée et remplacée. En cas de doute, prenez contact avec la BCJ.

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[1]. 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 ou un terminal de paiement 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 ou sur d'autres terminaux de paiement.
- 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.
- Demandez le blocage immédiat de votre carte si des anomalies sont constatées.
- Par défaut, votre carte Maestro est bloquée hors de la zone Europe. En cas de voyage dans le reste du monde, n'oubliez pas d'aviser la banque afin de débloquer la carte pour la zone concernée.

1 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

BCJ-Net

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 Internet security reconnu et d'un pare-feu (FireWall), assurez-vous qu'ils sont à jour et scannez fréquemment l'ordinateur.
- Evitez les connexions à partir d'un Wifi public non sécurisé.
- Passez toujours par le site 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 »).
- Utilisez l'application gratuite CrontoSign Swiss pour l'annonce au BCJ-Net ainsi que pour la validation d'un paiement (contrôlez les données du bénéficiaire et le montant).

Authentification par l'application CrontoSign Swiss

CrontoSign Swiss est une application gratuite en téléchargement gratuit sur App Store et Google Play qui vous permet une connexion au BCJ-Net. Elle permet de scanner une mosaïque, depuis l'appareil photo de votre smartphone ou via un lecteur optique. Ceci génère instantanément un code qui, une fois saisi sur le BCJ-Net, valide l'authentification ou le paiement non habituel. Ce nouveau procédé permet de crypter les données de login et les ordres en une mosaïque unique à chaque opération et pour chaque utilisateur.

Cette solution vous offre les avantages suivants :

Simplicité : l'application permet de photographier une mosaïque (cryptogramme au moyen de l'appareil photo de votre smartphone. Le code résultant permet une identification au BCJ-Net.
Rapidité : après installation et initialisation de l'application, le système est opérationnel immédiatement sur le téléphone portable, toujours à portée de main.
Sécurité : la signature systématique des paiements non habituels permet de rendre le trafic des paiements encore plus sûr.

BCJ Mobile banking

Sécurité

L'application BCJ Mobile banking bénéficie du même degré de sécurité que le BCJ-Net. Les données bancaires ne sont pas enregistrées sur votre appareil mobile.

Nos conseils de sécurité

- Assurez-vous de mettre régulièrement à jour votre système d'exploitation. Appliquez les mises à jour dès leur publication.
- Installez un antivirus sur votre appareil mobile (voir le site www.ebas.ch pour les recommandations)
- Télécharger uniquement les applications dont vous avez vraiment besoin.
- N'activez pas l'installation d'application provenant de source inconnue (paramètres de votre mobile).

Numéros d'urgence.

En cas de perte, vol ou blocage de carte.

Carte BCJ

+41 32 465 14 14 Service client 24h/24

Carte Maestro

+41 32 465 14 14 Service client 24h/24

Carte Visa / Mastercard

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

Carte TravelCash

+41 31 710 12 15 Perte ou vol de la carte

+41 31 710 11 11 Service client Swiss Bankers (lun - ven de 8h à 17h)

Support BCJ-Net

+41 32 465 13 01 Durant les heures d'ouverture de la banque

Labellisée Swiss Climate CO2 neutre, la BCJ s'engage pour l'environnement. Document imprimé sur papier 100% recyclé.

IP 0034 / 08-2017 / 2'000