Mobile Banking et Mobile Payment

Utilisez votre dispositif mobile pour payer, en toute sécurité !

Votre police et la Prévention Suisse de la Criminalité (PSC) – un organe intercantonal de coordination spécialisé de la Conférence des directrices et directeurs des départements cantonaux de justice et de police (CCDJP), en collaboration avec la Haute école spécialisée de Lucerne et « eBanking – en toute sécurité ! »

Vous effectuez déjà vos opérations bancaires sur votre tablette et à la caisse, vous préférez les paiements dématérialisés via smartphone ?

La banque mobile et les paiements mobiles représentent aujourd'hui deux des principales applications des dispositifs mobiles. Mais qu'en est-il de la sécurité et comment se prémunir contre d'éventuels préjudices financiers ?

Les avantages des dispositifs mobiles comme les smartphones et les tablettes sont évidents : pratiques, ils sont toujours à portée de main et connectés en permanence à Internet. Mais leur utilisation quotidienne présente les mêmes risques et dangers que ceux auxquels vous êtes exposé en utilisant votre ordinateur personnel. Les conseils qui suivent vous aideront à protéger au mieux votre dispositif mobile.

Maintenez votre dispositif mobile à jour et en parfait état de fonctionnement !

- **Installez uniquement des applications téléchargées depuis la plateforme officielle !** Ne téléchargez que des applications provenant d'Apple App Store ou Google Play Store. Méfiez-vous des applis mal notées par les utilisateurs. Avant de procéder à l'installation, renseignez-vous sur le fournisseur de l'application si vous ne le connaissez pas.
- **Procédez régulièrement aux mises à jour !** Activez la fonction des mises à jour automatiques sur votre dispositif mobile et installez sans attendre les correctifs de votre système d'exploitation et des applications installées. Désinstallez les applis obsolètes ou que vous n'utilisez plus, afin de vous protéger contre les risques.
- **Faites preuve de prudence lorsque vous ouvrez des messages provenant d'expéditeurs inconnus !** Ne cliquez sur aucun lien et ne téléchargez aucune pièce jointe provenant d'expéditeurs inconnus (qu'il s'agisse de mails, de messageries instantanées comme WhatsApp ou de MMS). Des logiciels malveillants (malwares) pourraient en effet s'y dissimuler. Installez une application antivirus sur votre dispositif Android. Ne vous inquiétez pas si vous ne trouvez pas d'antivirus pour dispositifs iOS : ils n'en ont pas besoin.
- **N'autorisez que les connexions nécessaires et fiables !** Votre dispositif mobile peut se connecter à Internet ou à d'autres appareils via Wifi/Wlan, NFC, Bluetooth, infrarouge, 3G/4G/5G etc. Activez uniquement le mode de connexion que vous souhaitez utiliser et n'acceptez aucune demande de connexion provenant d'appareils inconnus.

Respectez quelques règles de base lors de la configuration de votre dispositif mobile !

- **Limitez les droits d'accès de chacune de vos applications !** Pour chaque application, vérifiez quels sont les droits d'accès effectivement nécessaires à l'exécution de ses fonctionnalités et désactivez les droits qui ne le sont pas. Toutes les applis ne nécessitent pas forcément des droits d'accès complets, tels que l'accès aux données de géolocalisation, à la caméra ou aux contacts.
- **Soyez prudent quand il s'agit de communiquer votre position géographique !** Utilisez les services de localisation de façon judicieuse : n'associez pas de données de géolocalisation aux photos que vous publiez sur les réseaux sociaux par exemple.
- **Ne stockez pas de données confidentielles sur votre dispositif mobile ou sur le cloud !** Ne stockez jamais sur votre dispositif ou sur le cloud vos identifiants de connexion, tels que les codes PIN et TAN ou les mots de passe que vous utilisez dans le navigateur ou dans la plateforme d'applications. Ne stockez jamais vos identifiants sur votre dispositif ou sur le cloud. Utilisez un gestionnaire de mots de passe et désactivez l'enregistrement automatique des mots de passe sur votre dispositif mobile.

Protégez votre dispositif mobile contre les accès non autorisés !

- **Utilisez pour cela les paramètres de sécurité de votre appareil !** Activez le verrouillage d'écran. Utilisez pour cela un mot de passe fort, une empreinte digitale ou la reconnaissance faciale. Ne transmettez jamais vos données de connexion à qui que ce soit.
- **En cas de vol ou de perte, verrouillez immédiatement votre dispositif mobile !** Différentes applications permettent de verrouiller à distance les dispositifs perdus ou volés et d'empêcher quiconque d'accéder à vos données personnelles. Demandez à votre opérateur téléphonique de bloquer votre carte SIM.
- **Avant de le vendre ou de vous en débarrasser, pensez à rétablir les paramètres d'usine de votre smartphone !** Vous éviterez ainsi que les données stockées sur votre dispositif ne tombent entre de mauvaises mains. Retirez et détruisez également la carte SIM si vous ne vous en servez plus.

La banque mobile ou « Mobile Banking »

Le Mobile Banking consiste à effectuer des transactions bancaires à l'aide de dispositifs mobiles. Pour ce faire, les différents instituts financiers mettent à la disposition de leurs clients des applications mobiles ou un portail d'e-banking accessible depuis un navigateur. Le caractère mobile de ces services bancaires n'a aucune influence sur la sécurité, pour autant que l'on continue d'appliquer les règles de sécurité vues précédemment.

Mais dans le cas du Mobile Banking, il convient également ...

- **de choisir une connexion sécurisée.** En wifi, utilisez un chiffrement WPA2 ou WPA3 avec un mot de passe fort. Vous pouvez activer cette fonction sur votre routeur.
- **d'utiliser un autre dispositif séparé pour l'authentification bifactorielle.** Lorsque l'outil de banque mobile est utilisé depuis le dispositif mobile, on perd automatiquement le deuxième canal de communication indépendant nécessaire aux procédures mTAN et Photo-TAN. Pour remédier à ce problème, il convient d'utiliser un autre appareil mobile réservé à cet emploi, comme un vieux téléphone portable ou le dispositif TAN fourni par votre banque.

Le paiement mobile ou « Mobile Payment »

Le paiement mobile est une solution de paiement dématérialisé sans contact réalisé au moyen d'un dispositif mobile. La sécurité des paiements mobiles est souvent mise en cause. Que se passe-t-il au niveau des données personnelles ? La connexion est-elle sécurisée ? Les transactions sont-elles chiffrées ? L'important est que les données du client soient séparées de celles du paiement. Ainsi, l'exploitant de l'application utilisée (par exemple Twint ou Apple Pay) ne devrait jamais apprendre ce que le client a acheté, tout comme le commerçant ne devrait jamais avoir connaissance du solde que le client a sur son compte bancaire. Bien que cela soit difficile à vérifier, il est possible de clarifier cet aspect avec l'exploitant de l'application.

Pour sécuriser au mieux tous vos paiements mobiles, appliquez les règles de sécurité vues précédemment et ...

- **ne communiquez que les données véritablement nécessaires à l'application de paiement mobile.** Du point de vue de la protection des données, le danger réside dans la possibilité de relier les données de paiement et d'achat avec des données d'utilisation et de géolocalisation dans le but de créer des profils d'utilisateurs cohérents.
- **protégez l'accès à votre application de paiement mobile.** Activez les paramètres de sécurité de l'application. Configurez le verrouillage automatique au moyen d'un code, d'un mot de passe, d'une empreinte digitale ou de la reconnaissance faciale.

En savoir plus : **www.ebas.ch/mobilebanking**

Août 2022

SKPPSC

Prévention Suisse de la Criminalité
Maison des Cantons
Speichergasse 6
3001 Berne

www.skppsc.ch

Ce dépliant a été réalisé en collaboration avec la Haute école spécialisée de Lucerne et « eBanking – en toute sécurité ! »

www.ebas.ch | www.ebankingentoutesecurite.ch

HSLU Hochschule Luzern

eBanking en toute sécurité!