Les réseaux sociaux

Les réseaux sociaux comme Facebook, Instagram ou Youtube connaissent un succès fulgurant. À première vue, ceux-ci ne représentent pas directement un danger pour l'e-banking. Mais de par leur diffusion et leur utilisation souvent insouciante et inconsciente, ils ouvrent aussi des perspectives très juteuses aux criminels.

Pour vous protéger,

- ne publiez que des informations que vous pourriez confier à un inconnu rencontré dans la rue.
- limitez l'accès aux informations que vous publiez (options de confidentialité)
- n'acceptez dans votre cercle d'« amis » que les personnes que vous connaissez véritablement, personnellement ou à travers d'autres canaux.
- armez-vous de bon sens lorsque vous recevez les messages d'un inconnu.
- ne cliquez sur aucun lien provenant de sources inconnues et vérifiez tous les documents, images, vidéos etc. avant de les ouvrir.
- choisissez des mots de passe forts et utilisez un mot de passe différents pour chaque compte.
- veillez à ce que vos logiciels (navigateur, système d'exploitation, antivirus, etc.) soient toujours parfaitement à jour.

Les hackers adorent les réseaux sociaux

En positionnant de manière stratégique leurs liens piratés, les criminels utilisent souvent les réseaux sociaux comme « vecteur de propagation » de malwares.

Mais ils leur servent également à obtenir des informations personnelles sur les utilisateurs, informations qui pourront leur être utiles dans un deuxième temps pour une attaque ciblée.

Informations personnelles

Les réseaux sociaux sont basés sur le partage de photos et d'informations personnelles avec des « amis ». Or ces informations peuvent également être utilisées par un escroc dans le cadre par exemple d'une attaque d'ingénierie sociale ou « Social Engineering » (https://www.ebas.ch/fr/lingenierie-sociale-social-engineering/) .

Il importe donc de bien réfléchir aux informations que vous publiez sur votre profil. Dans les commentaires ou les statuts que vous publiez à votre sujet, limitez-vous aux informations personnelles que vous pourriez donner à un inconnu rencontré dans la rue.

En général, l'utilisation des réseaux sociaux nécessite une bonne dose de bon sens. Il convient ainsi de ne pas accepter les invitations des personnes que vous ne connaissez pas dans la vie réelle ou à travers d'autres canaux.

Avant d'être ouverts, tous les fichiers, qu'il s'agisse de documents, de photos, de vidéos ou autres, devraient toujours être analysés par un antivirus et ce, indépendamment de la fiabilité ou non de la source.

Publications et interactions

Sachez que les données personnelles que vous publiez, mais aussi toutes vos publications et interactions telles que les « J'aime », les partages etc. sont analysés par les opérateurs et agrégés dans un profil d'utilisateur (parfois défavorable, voire même faux) pour être par exemple vendues à des fins publicitaires. Les profils ainsi générés se diffusent rapidement sur d'autres réseaux sociaux, où ils peuvent rester pendant plusieurs années et sont souvent difficiles, pour ne pas dire impossibles à supprimer.

Par conséquent, dès lors qu'il s'agit de réseaux sociaux, il convient non seulement de faire preuve de réserve, mais aussi de bien réfléchir avant de communiquer quoi que ce soit.

Liens

Le simple fait de cliquer sur un lien renvoyant à un site Internet piraté suffit pour infecter votre dispositif avec un logiciel malveillant (Infection par drive-by download (https://www.ebas.ch/fr/infection-par-drive-by-download/)). Alors, avant de cliquer, demandez-vous si vous voulez vraiment afficher son contenu et posez-vous bien la question de la fiabilité de la source.

Le site www.getlinkinfo.com (http://www.getlinkinfo.com) permet de contrôler les liens raccourcis (cf. pour aller plus loin (#moreInfo)).

Il est par ailleurs indispensable que votre navigateur, votre système d'exploitation et votre programme antivirus soient parfaitement à jour, tout comme l'ensemble des applications et programmes installés (« Règle n°3 - Prévenir » (https://www.ebas.ch/fr/3-prevenir-avec-les-mises-a-jour-logicielles/)).

Identifiant et mot de passe

Vos comptes sur les réseaux sociaux doivent eux aussi être sécurisés par un mot de passe fort (https://www.ebas.ch/fr/4-proteger-les-acces-internet/) et vos identifiants personnels de connexion doivent absolument rester confidentiels.

Il est par ailleurs important d'utiliser des mots de passe différents pour chacun de vos comptes sociaux. **Dans tous les cas, évitez à tout prix d'utiliser le même mot de passe pour vos comptes sociaux et pour l'e-banking !**

Pour protéger le compte utilisateur d'un service donné, l'idéal serait d'utiliser, lorsque cela est possible, un système d'authentification à deux facteurs (https://www.ebas.ch/fr/4-proteger-les-acces-internet/) .

Protection des données

Le thème de la protection des données à caractère personnel revêt une importance capitale dès lors qu'il s'agit de réseaux sociaux et de leur utilisation. Vous trouverez à ce propos une foule d'informations et de conseils pratiques sur le site Internet du Préposé fédéral à la protection des données et à la transparence (PFPDT) (https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz.html) .

Paramètres recommandés

Les réseaux sociaux offrent de nombreuses possibilités de configuration. Nos check-lists vous aideront à sécuriser au mieux vos profils Facebook (https://www.ebas.ch/fr/parametres-facebook/) , Twitter (https://www.ebas.ch/fr/parametres-twitter/) , Instagram (https://www.ebas.ch/fr/parametres-instagram/) et LinkedIn (https://www.ebas.ch/fr/parametres-linkedin/) en jouant sur les paramètres.

Affirmer que les réseaux sociaux n'ont rien à voir avec la sécurité en e-banking serait une erreur, dans la mesure où ils représentent une source d'informations non négligeable pour les arnaqueurs.

Côté utilisateurs, quelques mesures efficaces suffisent pour profiter sereinement de ces nouveaux outils de communication.

Mémento : *Download (PDF) (https://www.ebas.ch/wp-content/uploads/2020/01/socialmediaSKP_fr.pdf)*

Pour aller plus loin

Certains réseaux sociaux limitent la longueur maximale des messages pouvant être publiés. Twitter par exemple impose une limite de 280 caractères à ses utilisateurs. D'où l'intérêt des différents réducteurs de lien qui permettent de transformer des URL trop longues en des liens beaucoup plus courts et donc plus faciles à partager. Un raccourcisseur de lien permet ainsi de transformer par exemple l'URL

« https://www.ebas.ch/de/ihrsicherheitsbeitrag/erweiterter-schutz/114-socialengineering »

en

« http://bit.ly/P4u765 »

Ce nouveau lien raccourci ne permet plus de vérifier visuellement la cible à laquelle il renvoie. Les hackers peuvent justement en profiter pour dévier les internautes vers des sites Internet piratés.

Voilà pourquoi il convient de vérifier l'adresse URL d'origine avant de cliquer sur un lien raccourci. Ce service est offert par le site www.getlinkinfo.com (https://www.getlinkinfo.com) qui permet également d'obtenir, en plus de l'adresse d'origine, des informations supplémentaires sur le site en question.