Autoriser ou non l’accès d’opérateurs tiers à ses comptes bancaires

Différents opérateurs tiers offrent aux utilisateurs de l’-e-banking des services interbancaires de paiement et d'information sur leurs comptes. Pratiques, ces services présentent néanmoins un certain nombre de risques.

Pour vous protéger,

- Ne communiquez jamais vos identifiants personnels de connexion pour l’e-banking (mot de passe, code PIN, numéro d'identification, etc.), qu'il s’agisse d'une personne ou d'un service offert par un opérateur tiers.

Pour accéder aux comptes bancaires, les opérateurs tiers demandent et utilisent la plupart du temps les identifiants de connexion à l’e-banking des clients. Or, en transmettant vos identifiants personnels à des tiers, vous vous exposez en tant que client à d’énormes risques de sécurité. De plus, le passage des systèmes très réglementés des instituts financiers suisses (FINMA, loi sur les banques, etc.) aux environnements beaucoup moins régulés des opérateurs tiers comporte des risques pour vos données bancaires.

Soyez prudent !

L'usurpation d'identité, de même que le traitement et le stockage non réglementé des données bancaires clients représentent des risques importants pour vous.

«eBanking – en toute sécurité!» conseille par conséquent de ne jamais transmettre à des tiers ses identifiants personnels de connexion aux services d’e-banking.

Copyright © 2024 – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique

Pour aller plus loin

Les risques liés à l'utilisation des services interbancaires en ligne

Parmi les différents services offerts par les opérateurs tiers utilisant les identifiants personnels de connexion à l'e-banking des clients, il y a par exemple les plateformes d'accès uniques aux comptes bancaires de différents instituts financiers. Mais attention : sachez qu'en transmettant à une telle plateforme vos identifiants personnels de connexion à l'e-banking, vous courrez un énorme risque de sécurité.

L'usurpation d'identité, un risque de sécurité à prendre au sérieux

Pour accéder aux comptes bancaires de leurs clients, les opérateurs tiers ont souvent recours à ce que l'on appelle l'usurpation d'identité. Ils demandent donc à leurs clients de leur fournir leurs identifiants personnels de connexion (ex. mot de passe et numéro d'identification) afin d'obtenir un accès illimité à ces comptes.

À partir du moment où vous communiquez, en tant que client, vos identifiants personnels de connexion, vous agissez en quelque sorte comme si, au moment de régler votre forfait vacances dans une agence de voyages, vous ouvriez votre session d'e-banking sur l'ordinateur de votre agent et que vous quittiez le magasin en lui faisant absolument confiance sur le montant à débiter. Sans parler du fait qu'avant de fermer votre session, il pourrait en profiter par exemple pour regarder le montant du salaire que vous recevez chaque mois, et pourquoi pas utiliser votre compte pour financer ses propres vacances. D'un point de vue technique, l'usurpation d'identité s'apparente à une attaque classique de phishing (https://www.ebas.ch/fr/le-phishing/) , même lorsqu'il s'agit d'un opérateur tiers sérieux.

Pour l'institut financier, il est difficile de savoir dans ces conditions s'il communique avec vous en tant que client ou avec un prestataire tiers agissant en votre nom ou – dans le pire des cas – avec un intermédiaire malveillant. L'institut financier n'est alors plus en mesure de remplir correctement ses devoirs de diligence, comme par exemple celui de protéger les données bancaires de ses clients. Et en cas de dommages, vous risquez même de tomber sous le coup des clauses d'exclusion de responsabilité.

Perte de contrôle des données bancaires clients

Alors que les instituts financiers suisses sont soumis à des règles très strictes pour la protection des données bancaires de leurs clients et la sécurité de leurs systèmes, les opérateurs tiers peuvent, avec votre autorisation, stocker et traiter des données dans des environnements et des systèmes moins réglementés. Les opérateurs tiers ne sont pas toujours les propriétaires et n'ont pas toujours le contrôle de ces systèmes. Ils utilisent en effet souvent des solutions de Cloud, la plupart du temps sans savoir vraiment avec précision où les données se trouvent stockées. Le secret bancaire suisse ne vaut généralement pas pour ces systèmes !

La perte de contrôle sur le stockage des données personnelles a des répercussions difficiles à évaluer. Ce qui est sûr, c'est que cela facilite la tâche des hackers qui veulent accéder aux données bancaires personnelles des clients.

Copyright © 2024 – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique