E-Banking

Reconnaître les arnaques courantes

Faire la queue dans une banque appartient au passé. Aujourd'hui, il est possible de faire toutes ses opérations financières depuis l'ordinateur familial. En quelques secondes, on peut consulter son solde pour savoir combien d'argent il reste pour faire les boutiques, ou effectuer un virement en un seul clic – tout cela ne pose aujourd'hui plus aucun problème. Ou peut-être que si? De plus en plus d'escrocs se sont donné comme but de voler, utiliser ou même de revendre des données. Le business avec les données et l'argent volés a le vent en poupe.

L'hameçonnage (Phishing)

Lors de l'hameçonnage, les escrocs essaient à l'aide de sites Web copiés de vous inciter à saisir vos données bancaires dans le but de vider votre compte.

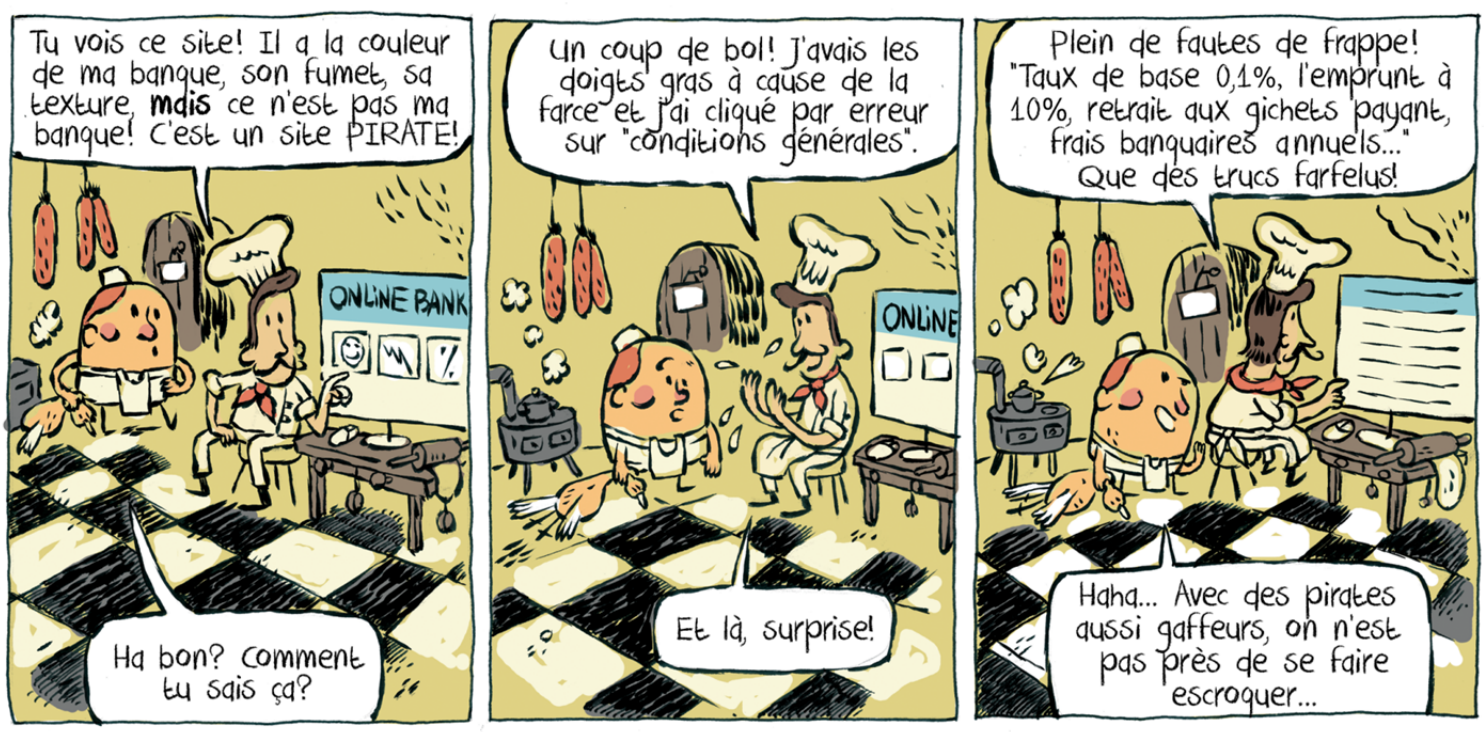
Un des nombreux scenarii possibles: vous recevez un e-mail de votre banque ou d'un autre service en ligne auprès duquel vous êtes inscrit. Il en ressort qu'il y aurait un problème avec votre compte. De quel problème il s'agit vraiment n'est pas expliqué. Il vous est demandé de vous connecter d'urgence à votre compte afin "d'éviter le pire". Pratique : l'e-mail comprend le lien correspondant. Il suffit de cliquer sur le lien pour accéder à une page sur laquelle vous devez vous connecter.

Le problème: la page à laquelle vous accédez via le lien ressemble fortement à l'équivalent officiel mais il s'agit en réalité d'un faux. Toutes les données que vous y saisissez seront enregistrées par des escrocs et seront ensuite utilisées ou vendues à des fins criminelles.

Ne cliquez jamais sur les liens contenus dans les e-mails qui prétendent avoir été envoyés par votre banque. Les banques luxembourgeoises n'envoient pas d'e-mails vous demandant de saisir vos données.

Ne saisissez jamais des informations personnelles dans des formulaires qui arrivent par e-mail.

De manière générale, ne répondez pas aux e-mails qui vous demandent de communiquer des informations confidentielles ou personnelles.



Examinez les e-mails d'un œil critique. Soyez prudent lorsque:

- *un e-mail vous met sous pression et vous demande de réagir vite*
- *un e-mail vous demande de cliquer sur un lien afin d'accéder à un site Web où vous devez saisir vos données*
- *un e-mail n'est pas adressé à vous personnellement ou dont le texte comporte de nombreuses fautes ou une très mauvaise traduction (un e-mail adressé personnellement à vous n'est toutefois pas une garantie de fiabilité!)*

Cheval de Troie bancaire

Il existe de nombreuses variantes de chevaux de Troie. Ils ont tous une chose en commun : ils s'exécutent en arrière-plan et vident votre compte sans que vous vous en rendez immédiatement compte. Lors d'une session de web banking ouverte, les criminels effectuent des virements que vous ne voyez pas. Le solde du compte ne change pas, et même dans le historique des virements, le cheval de Troie ne laisse aucune trace visible grâce à une programmation sophistiquée. Mais votre argent disparaît tout de même !

Le cheval de Troie bancaire est un logiciel malveillant qui est diffusé via les moyens d'infection habituels (p.ex. comme pièce jointe ou lien avec un e-mail, en profitant d'une faiblesse du programme informatique). Il reconnaît de manière autonome lorsque vous vous connectez à la page de web banking et le signale à son créateur criminel. Celui-ci peut alors prendre le contrôle de votre compte tant que votre session est ouverte.

Ne téléchargez jamais des fichiers joints à des e-mails ou disponibles sur des sites Web, dont vous ne connaissez ni leur source ni leur but. Maintenez toujours tous vos logiciels et plug-ins à jour. Déconnectez-vous toujours à l'aide du bouton prévu à cet effet des sites Web de banque en ligne. Il ne suffit pas de fermer la fenêtre du navigateur, car cela ne permet pas de clôturer votre session qui reste donc accessible aux criminels.

Une version de cheval de Troie bancaire envoie à sa victime un message l'informant que la banque lui aurait viré par erreur une somme d'argent élevée. En réalité, le visuel du compte de la victime a été manipulé : en effet, il semble qu'une grosse somme d'argent ait été versée sur votre compte. Si la victime reverse l'argent versé par erreur, celui-ci sera réellement débité de son propre capital. Méfiez-vous donc toujours des messages de ce type et en cas de doute, contactez directement votre banque.

Si vous constatez que votre compte a été piraté, contactez immédiatement votre banque et la police.

Le plus sûr, est de respecter ces règles de comportement concernant la banque en ligne (e-banking):

- Ne pas transmettre de données bancaires suite à un e-mail (les banques luxembourgeoises ne font jamais de telles demandes par mail)
- Ne jamais se logger à son compte en banque à partir d'un ordinateur étranger ou public
- Utiliser des authentifications fortes (produits LuxTrust) pour le web-banking
- Se déconnecter correctement de son accès web-banking : il ne suffit pas de fermer la fenêtre du navigateur !
- Garder son compte bancaire à l'œil pour signaler sans tarder des débits illégitimes
- Vérifier que la page soit chiffrée après la connexion (https)
- Conservez les mots de passe en lieu sûr et idéalement de manière chiffrée
- Si vous rencontrez des anomalies pendant votre session d'e-banking ou si vous constatez des failles de sécurité, informez-en immédiatement votre banque.

Pour toute question au sujet de l'arnaque en ligne ou sur l'utilisation d'Internet en général, contactez la BEE SECURE Helpline :

BEE SECURE HELPLINE
CONSEIL & AIDE
8002-1234

Éditeur : BEE SECURE · B.P. 707 · L-2017 Luxembourg
Tel.: (+352) 247-86427 · Fax.: (+ 352) 46 41 86
bee-secure@snj.lu · www.bee-secure.lu

THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
Co-funded by the European Union