Services bancaires en ligne sécurisés

Si les règles de sécurité suivantes sont respectées, effectuer des transactions bancaires en ligne s'avère sûr et pratique :

Authentification à 2 facteurs

L'authentification fonctionne selon le principe de combinaison : quelque chose que vous savez (mot de passe) et quelque chose que vous possédez.

Lors de la connexion avec le compte bancaire en ligne, l'utilisateur doit encoder son numéro «PIN» (= numéro d'identification personnel, angl.: Personal Identification Number) ou confirmer sa transaction avec un «TAN» (= numéro d'authenfication de transaction, angl.: Transaction Authenfication Number) en plus de son mot de passe. Il s'agit d'une combinaison de chiffres variables, qui peut, par exemple, être générée par un «TOKEN». Les banques proposent différentes méthodes.

Il existe divers produits assurant une authentification forte pour effectuer des transactions en ligne. Au Luxembourg, les produits LuxTrust sont utilisés par de nombreuses banques et administrations publiques.

HTTPS

Si des données confidentielles sont transmises sur Internet, l'utilisateur doit toujours veiller à ce qu'un cadenas ou une clé soit affichée dans la barre d'adresse du navigateur. Par conséquent, l'adresse Internet commence avec «https**s**» au lieu de «http». Le «s» signifie «sécurité» (ou plus précisément «chiffrement») et les données échangées ne peuvent pas être altérées ni lues par des tiers.

Les transactions bancaires en ligne et toutes autres transactions financières doivent toujours être effectuées avec une connexion «https».

Ordinateur séparé

Idéalement, il faudrait un ordinateur distinct pour les transactions bancaires en ligne, qui serait utilisé uniquement à cette fin et sur lequel aucune autre activité en ligne ne serait effectuée. Si vous n'avez pas la possibilité de réserver un ordinateur aux transactions bancaires, utilisez au moins un navigateur différent de votre navigateur habituel. D'une manière générale, réduisez les risques d'infection liés aux activités en ligne.

Aucune transaction financière ne doit être effectuée à partir d'un ordinateur public et / ou sur des réseaux publics.

Courriel

Généralement, les institutions financières réputées ne sollicitent pas les informations de connexion ou d'autres informations confidentielles par e-mail. En outre, il ne faut JAMAIS cliquer sur les liens dans les courriels qui prétendent provenir d'une banque. Ces liens conduisent souvent à de faux sites Web qui sont utilisés à des fins criminelles. En cas de doute, informez votre agence bancaire par téléphone.

Contrairement aux banques, les services de paiement en ligne, tels que *PayPal*, envoient des e-mails à leurs clients. De ce fait, les cybercriminels envoient régulièrement des mails usurpateurs dans le but d'extorquer les données de connexion des clients de *Paypal*.

Mises à jour

Tant le navigateur que le logiciel anti-virus et les autres programmes doivent être mis à jour régulièrement. Les mises à jour servent notamment à supprimer les failles de sécurité qui sont décelées. Au Luxembourg les services bancaires en ligne sont effectués presque exclusivement sur Java, ce logiciel est donc une cible fortement visée par les cybercriminels.

Les utilisateurs du e-banking doivent veiller à ce que la dernière version Java soit installée sur leur ordinateur.

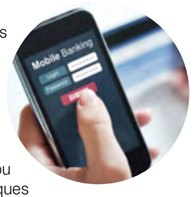
WLAN sécurisé

En général, les transactions financières devraient être uniquement effectuées à partir de la connexion Wi-Fi privée de l'utilisateur. Celle-ci doit être protégée par un mot de passe fort. Cela vaut également pour le routeur. Les mots de passe par défaut doivent être modifiés.

En général un mot de passe doit :

- être unique : 1 mot de passe pour 1 application ou service en ligne ;
- compter au moins 12 caractères et être composé de chiffres, de lettres majuscules et minuscules ainsi que de caractères spéciaux ;
- rester secret.

Mobile Banking



Pour effectuer des transactions bancaires via son smartphone ou sa tablette, il convient de protéger son appareil avec une application de sécurité. Les applications bancaires doivent être téléchargées uniquement sur les plateformes officielles comme Apple Store ou Google Play. La plupart des banques offrent maintenant des applications bancaires pour leurs clients, ainsi que diverses procédures TAN.

Pour les services bancaires mobiles il faut éviter que les codes TAN soient envoyés par SMS sur l'appareil utilisé pour accéder au e-banking. PIN, TAN, mots de passe et données d'accès ne doivent être stockés ni sur l'ordinateur, ni sur le smartphone.

Les mêmes règles sont applicables pour les services bancaires en ligne par l'intermédiaire d'un ordinateur fixe ou portable.

Se déconnecter

Après avoir accédé à un site e-banking, il convient de se déconnecter manuellement en cliquant sur le bouton «déconnexion». Attention, il ne suffit pas de «fermer» la page du browser pour terminer la connexion.

Internet en sécurité Les règles d'or

1 Cliquer malin

Les escroqueries en ligne peuvent être coûteuses. Restez vigilant et prenez votre temps. En cas de doute, mieux vaut ne pas cliquer.

2 Utiliser des mots de passe forts

Un mot de passe contient au moins 12 caractères et est composé de chiffres, de lettres majuscules et minuscules, ainsi que de caractères spéciaux. Utilisez un mot de passe différent pour chaque sites ou applications.

3 Protéger l'identité

Plus les informations que vous divulguez sur Internet sont personnelles, plus elles sont attrayantes, voire lucratives pour les cybercriminels. Ainsi, ne donnez que le minimum d'informations lorsque celles-ci ne sont pas nécessaires.

4 Faire des mises à jour régulières

Les mises à jour consistent à corriger les lacunes de sécurité dans les programmes. Assurez-vous que les logiciels et les extensions soient actualisés.

5 Protéger l'ordinateur

Un logiciel anti-virus et un pare-feu activé sont absolument essentiels.

6 Sauvegarder les données

Pour éviter de perdre vos fichiers et données en cas d'incident, des sauvegardes doivent être effectuées régulièrement.

Pour plus d'explications détaillées, instructions et autres conseils :
www.silversurfer.lu

Notice légale

Cette publication a été réalisée par le SNJ (Service National de la Jeunesse) dans le cadre du projet BEE SECURE.

Tirage: 1000 exemplaires
Sicheres Online-Banking v.2 - 02/2018

Sicheres Online-Banking

BEE SECURE silversurfer.lu

RBS | CENTER FIR ALTERSFROEN | ASSR

Co-financed by the European Union
Connecting Europe Facility

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Famille, de l'Intégration et à la Grande Région

Sicheres Online-Banking

Online Banking ist bequem und sicher, wenn nachstehende Sicherheitsregeln befolgt werden:

Zwei-Faktor-Authentifizierung

Die Authentifizierung funktioniert nach dem Kombinationsprinzip: Etwas, das man weiß (Passwort) und etwas, das man besitzt.

Bei der Anmeldung beim Online-Bankkonto muss der Benutzer neben seinem konstanten Passwort eine PIN-Nummer (=Persönliche Identifikationsnummer, engl.: Personal Identification Number) eingeben oder die Transaktionen mit einer sogenannten TAN-Nummer (=Transaktionsnummer, engl.: Transaction Authentification Number) bestätigen. Es handelt sich um eine zufällige Nummer die z.B. über ein sogenanntes TOKEN generiert wird. Die Banken bieten verschiedene Verfahren an.

Es existieren verschiedene Produkte die eine starke Authentifizierung für Online-Transaktionen versichern. In Luxemburg verwenden Banken und öffentliche Ämter vorwiegend LuxTrust-Produkte.

HTTPS

Wenn im Internet vertrauliche Daten übermittelt werden, sollte der Benutzer stets darauf achten, dass in der Adress-Zeile im Browser entweder ein Vorhängeschloss oder ein Schlüssel angezeigt wird. Die Internetadresse beginnt dann folglich mit „https“ anstatt „http“. Das „s“ steht für sicher und bedeutet, dass die Verbindung nicht kompromittiert oder mitgelesen werden kann.

Online-Banking und andere Geldtransaktionen sollen ausschließlich über eine „https“-Verbindung erledigt werden.

Separater Computer

Im Idealfall sollte für Online-Banktransaktionen ein separater Computer gebraucht werden, der nur zu diesem Zweck benutzt wird und auf dem keine weiteren Internet Aktivitäten stattfinden. Steht ein solcher nicht zur Verfügung, sollte wenigstens ein anderer Browser gebraucht werden, als der für die üblichen Online-Aktivitäten. Je weniger Internet-Aktivitäten stattfinden - dazu gehört auch E-Mailing – umso geringer die Virus-, resp. Trojaner-Gefahr.

Grundsätzlich sollen keine Geldtransaktionen an einem fremden Computer und/oder in öffentlichen Netzwerken erledigt werden.

E-Mails

Grundsätzlich gilt: Seriöse Geldinstitute fordern keine Zugangsdaten oder sonstige vertrauliche Informationen per E-Mail! Des weiteren sollte NIEMALS auf Links in E-Mails geklickt werden, die vorgeben von einer Bank zu sein. Diese Links leiten oft auf gefälschte Webseiten, die zu kriminellen Zwecken genutzt werden. Im Zweifelsfall sollte die Bankfiliale telefonisch informiert werden.

Online-Bezahldienste, wie *Paypal*, verschicken – im Gegensatz zu Banken – schon mal E-Mails an ihre Kunden. Diese Tatsache wird gerne von Cyberkriminellen missbraucht und unter falschen, jedoch täuschend echten Vorgaben für Phishing Mails genutzt.

Updates

Sowohl die Browser, als auch die Antivirensoftware und sonstige Programme sollten regelmäßig aktualisiert werden. Updates dienen vorwiegend der Schließung von Sicherheitslücken, um einen effektiveren Schutz zu gewährleisten. Da in Luxemburg Online-Banking fast ausschließlich über die Software Java ausgeführt wird, ist diese ein begehrtes Angriffsziel von Cyberkriminellen.

E-Banking User sollten unbedingt darauf achten, dass auf ihrem Computer jeweils die neueste Version von Java installiert ist.

Gesichertes WLAN

Geldtransaktionen sollten generell nur über das eigene WLAN getätigt werden. Dies sollte mit einem starken Passwort geschützt sein. Das Gleiche gilt für den Router.

Wenn möglich sollte das vom Internetanbieter voreingestellte Router-Passwort geändert werden.

Allgemein sollen Passwörter:

- Einmalig sein.: Für verschiedene Zwecke – verschiedene Passwörter
- Mindestens 12 Zeichen lang und aus Zahlen, großen und kleinen Buchstaben sowie Sonderzeichen bestehen.
- Nicht offensichtlich aufbewahrt werden und/oder an Dritte weitergegeben werden.

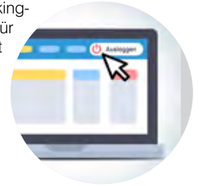
Mobile Banking

Wer Bankgeschäfte über sein Smartphone oder Tablet abwickeln will, sollte sein Gerät mit einer Sicherheits-Software schützen. Banking-Apps sollten nur von offiziellen Plattformen wie Google Play oder Apple Store herunter geladen werden. Die meisten Geldinstitute bieten Banking-Apps für ihre K sowie verschiedene TAN-Verfal

Beim Mobile-Banking sollte unbedingt vermieden werden, dass TAN Codes per SMS auf demselben Gerät empfangen werden, mit dem auch Überweisungen getätigt werden. PIN, TAN, Passwörter und Zugangsdaten sollten weder auf dem Computer, noch auf dem Smartphone gespeichert werden.

Ansonsten gelten dieselben Regeln wie fürs Online-Banking über einen Laptop oder Rechner.

Ausloggen



Die Verbindung mit einer E-Banking-Seite sollte immer über das dafür vorgesehene Logout-Menü beendet werden. Die Seite „nur“ schließen reicht nicht aus um die Verbindung definitiv zu unterbrechen.

Sicher im Netz – Die goldenen Regeln

1 Clever klicken

Online-Betrug kann teuer werden. Bleiben Sie wachsam und lassen Sie sich Zeit. Im Zweifelsfall besser nicht anklicken.

2 Starke Passwörter benutzen

Ein starkes Passwort ist mindestens 12 Zeichen lang und besteht aus Zahlen, großen und kleinen Buchstaben sowie Sonderzeichen. Für verschiedene Zwecke sollten verschiedene Passwörter benutzt werden.

3 Identität schützen

Je mehr persönliche Daten Sie im Internet preisgeben, um so attraktiver und ggf. auch lukrativer werden Sie für Cyberkriminelle. Geben Sie also nur die nötigsten Informationen preis, falls erforderlich.

4 Regelmäßig Programme aktualisieren

Updates schließen Sicherheitslücken in Programmen. Vergewissern Sie sich, dass alle Programme und „Plugins“ immer auf dem letzten Stand sind.

5 Den Computer schützen

Ein Anti-Virus Programm und eine aktivierte Firewall sind unbedingt erforderlich.

6 Daten sichern

Damit im Ernstfall keine Daten verloren gehen, sollten regelmäßig Sicherungskopien angefertigt werden.

Ausführliche Erklärungen, Anweisungen und weitere Tipps auf:
www.silversurfer.lu

Notice légale

Cette publication a été réalisée par le SNJ (Service National de la Jeunesse) dans le cadre du projet BEE SECURE.

Tirage: 1000 exemplaires
Sicheres Online-Banking v.2 - 02/2018

Services bancaires en ligne sécurisés

BEE SECURE silversurfer.lu

RBS CENTER FIR ALTERSFROEN ASSB

Co-financed by the European Union
Connecting Europe Facility

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Famille, de l'Intégration et à la Grande Région