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.

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 Kunden an, sowie verschiedene TAN-Verfahren.

! 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.

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.

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.

! *Paypal* ist die einzige Luxemburger Bank die E-Mails an ihre Kunden verschickt. Diese Tatsache wird gerne von Cyberkriminellen missbraucht und unter falschen, jedoch täuschend echten Vorgaben für Phishing Mails genutzt.

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.

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

Sicheres Online-Banking

silversurfer.lu

SECURITY MADE IN.LU

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

RBS CENTER FIR ALTERSFROEN

ASSB

BEE SECURE