E-Banking

Gängige Betrugsmaschen erkennen

In der Bank Schlange stehen war gestern. Heute kann man alle seine Finanzangelegenheiten bequem vom heimischen Computer aus erledigen. In Sekundenschnelle nachsehen, wieviel Geld einem noch bleibt, um shoppen zu gehen, oder schnell eine Überweisung tätigen – all das ist heute kein Problem mehr. Oder etwa doch? Immer mehr Betrüger haben es sich zur Aufgabe gemacht, Daten zu stehlen, zu benutzen oder sogar weiterzuverkaufen. Das Geschäft mit den geklauten Daten und dem geklauten Geld läuft besser denn je.

Phishing

Beim Phishing versuchen Betrüger, Sie mit Hilfe von kopierten Internetseiten zur Eingabe Ihrer Bankdaten zu verleiten, um anschließend Ihr Konto zu plündern. Eines von vielen möglichen Szenarien: Sie erhalten eine E-Mail von Ihrer Bank oder einem anderen Online-Dienst, bei dem Sie angemeldet sind. Daraus geht hervor, dass es offensichtlich Probleme mit Ihrem Konto gibt. Was genau passiert ist, bleibt unklar. Dringend werden Sie jedoch dazu aufgefordert, sich in Ihren Account einzuloggen, um „das Schlimmste zu verhindern“. Praktisch, dass der Absender den passenden Link gleich mitliefert. Sie brauchen ihn nur noch anzuklicken und gelangen gleich auf eine Seite, auf der Sie sich einloggen sollen.

Das Problem dabei: Die Seite, auf die Sie über den Link gelangen, sieht ihrem offiziellen Pendant zwar täuschend ähnlich, ist aber gefälscht. Alle Daten, die Sie hier eingeben, werden von Kriminellen gespeichert und anschließen für kriminelle Zwecke verwendet bzw. verkauft.

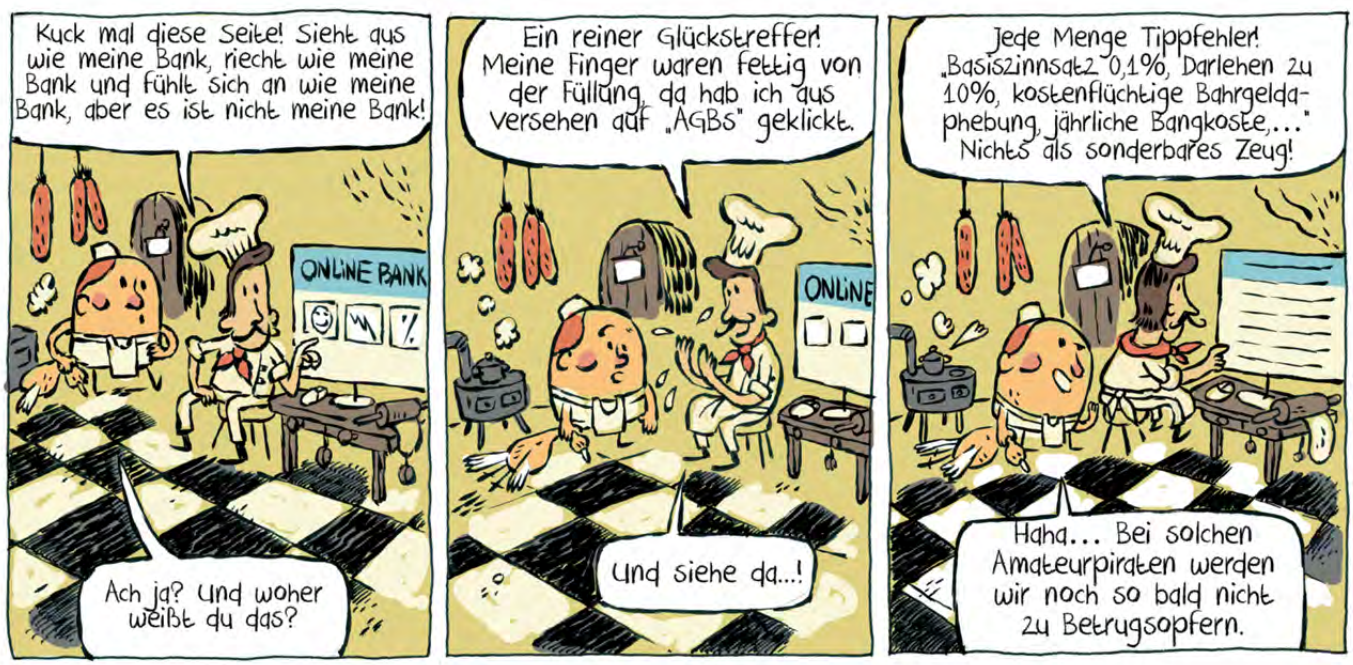
Klicken Sie nicht auf Links in E-Mails, die vorgeben, von Ihrer Bank zu sein. Luxemburgische Banken verschicken keine E-Mails mit der Aufforderung zur Eingabe von Daten.

Geben Sie keine personenbezogenen Informationen in Formulare ein, die per E-Mail eintreffen.

Antworten Sie generell nicht auf E-Mails, in denen vertrauliche oder personenbezogene Informationen angefordert werden.

Prüfen Sie jede E-Mail kritisch. Besondere Vorsicht gilt, wenn:

- Eine E-Mail Sie unter Druck setzt, schnell zu reagieren
- Eine E-Mail Sie dazu auffordert, einen Link anzuklicken, um auf eine Webseite zu gelangen, wo Sie Ihre Daten eingeben sollen
- Eine E-Mail nicht an Sie persönlich gerichtet ist oder viele Schreibfehler, bzw. eine sehr schlechte Übersetzung enthält (Wobei auch eine persönliche Anrede kein Garant für eine vertrauenswürdige E-Mail ist!)



Banking-Trojaner

Banking-Trojaner gibt es in unzähligen Variationen. Was sie alle gemeinsam haben: Sie laufen im Hintergrund und plündern Ihr Konto, ohne dass Sie direkt etwas davon mitbekommen. Während einer offenen Web-Banking-Sitzung tätigen die Kriminellen Überweisungen, die Sie nicht sehen. Der Kontostand ändert sich nicht, und auch im Überweisungsverlauf hinterlässt der Trojaner dank ausgeklügelter Programmierung keine sichtbaren Spuren. Ihr Geld ist trotzdem weg!

Der Banking-Trojaner ist ein Schadprogramm, das über die üblichen Infektionswege verbreitet wird (z.B. als Attachment oder Link in E-Mails, durch Ausnutzen einer Schwachstelle im Computerprogramm). Es erkennt eigenständig, wenn Sie sich in Ihre Web-Banking-Seite einloggen und meldet dies an seinen kriminellen Erschaffer. Dieser hat nun seinerseits freie Kontrolle über Ihr Konto, solange Ihre Sitzung offen ist.

Laden Sie keine Dateien aus E-Mails oder von Webseiten herunter, deren Herkunft und Zweck Ihnen nicht bekannt sind. Halten Sie alle Ihre Programme und Plugins stets auf dem neusten Stand. Loggen Sie sich immer mithilfe des dafür vorgesehenen Buttons aus Banking-Webseiten aus. Es reicht nicht, einfach nur das Browserfenster zu schließen, denn damit ist Ihre Sitzung noch nicht beendet und kann von Kriminellen weiter ausgenutzt werden.

Eine Version des Banking-Trojaners schickt ihrem Opfer eine Benachrichtigung, die Bank habe ihm fälschlicherweise eine hohe Geldsumme überwiesen. In Wahrheit wurde jedoch die Kontoansicht des Opfers manipuliert: Es sieht tatsächlich so aus, als befände sich die angesprochene Geldsumme auf dem Konto. Überweist das Opfer das vermeintlich unrechtmäßig erhaltene Geld zurück, geht das vom eigenen Kapital ab. Seien Sie deshalb immer skeptisch bei Benachrichtigungen dieser Art und rufen Sie im Zweifelsfall direkt Ihre Bank an.

Wenn Sie feststellen, dass Ihr Konto gehackt wurde, kontaktieren Sie unverzüglich Ihre Bank und die Polizei.

Am sichersten sind Sie, wenn Sie unsere E-Banking-Verhaltensregeln beherzigen:

- Niemals vertrauliche Informationen aufgrund einer E-Mail preisgeben
- Nicht auf Links in E-Mails klicken, die vorgeben, von Ihrer Bank zu sein
- Die Bankkonten im Auge behalten und regelmäßig auf irreguläre Abbuchungen überprüfen
- Aus Banking-Webseiten richtig ausloggen
- Benutzen Sie die LuxTrust-Produkte zur sicheren Authentifizierung
- Vergewissern Sie sich, dass die Seite nach dem Anmelden verschlüsselt ist (https)
- Niemals von einem fremden Rechner aus in eine Bankwebseite einloggen!
- Passwörter sicher (am besten verschlüsselt) verwahren und niemals einer anderen Person mitteilen
- Wenn Sie während Ihrer E-Banking / E-Commerce-Sitzung Anomalien oder Sicherheitsrisiken bemerken, melden Sie dies unverzüglich Ihrer Bank

Sollten Sie Fragen zum Thema Online-Betrug oder zur Internetnutzung generell haben, kontaktieren Sie die BEE SECURE Helpline:

BEE SECURE HELPLINE
BERATUNG & HILFE
8002-1234

Herausgeber: 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