„Wie funktioniert Online-Banking sicher“

Am 23. Januar 2019 trafen sich 18 Bikultler im PC-Raum der Alten Schule am Heideweg, um sich über die Sicherheit und Handhabung im Umgang mit dem Online-Banking zu informieren.

Dazu bekamen wir professionelle Hilfe von Frau Sabrina Bick und Herrn Yannik Schulze von der Sparkasse Filiale Belm. Viele von den heutigen Teilnehmern nutzen bereits zur Abwicklung ihrer Bankgeschäfte das Online-Banking. Dafür gibt es verschiedene Zugangsmedien.

Zur Abwicklung von Bankgeschäften mittels Online-Banking unter Verwendung von PIN und TAN benötigt der Nutzer zunächst eine persönliche Identifikationsnummer (PIN) und gegebenenfalls eine Transaktionsnummer (TAN) aus einer TAN-Liste, aus einer chip-TAN oder einer sms-TAN. Der Kunde hat mittels Online-Banking Zugang zum Konto/Depot, wenn er zuvor seine Konto/Depotnummer und seine PIN eingegeben hat. Eventuell hat der Nutzer jeweils eine zusätzliche TAN einzugeben. Außerdem ist der Nutzer verpflichtet die tech-nische Verbindung zum Online-Banking-Angebot über die Online-Banking Zugangskanäle herzustellen. Nach erfolgtem Zugang kann der Kunde z.B. Überweisungen tätigen, die allerdings zusätzlich der Eingabe einer TAN bedarf. Diese TAN-Nummer kann man anschließend nicht wieder verwenden. Selbstverständlich hat der Kunde bzw. Nutzer dafür Sorge zu tragen, dass keine andere Person Kenntnis von PIN und TAN erlangt, denn sonst könnte diese Person Aufträge zu Lasten des Kontos/Depots erteilen. PIN und TAN dürfen nicht elektronisch gespeichert oder in anderer Form notiert werden. Bei Eingabe von PIN und TAN muss sichergestellt sein, dass Dritte von dieser keine Kenntnis erlangen können. Hat man festgestellt, dass Missbrauch getrieben worden ist, so ist der Kunde verpflichtet unverzüglich seine PIN zu ändern und die restlichen TANs aus der Liste zu sperren. Ab Zugang der Sperrmeldung haftet das Kreditinstitut für alle Schäden, die durch Nichtbeachtung entstehen.

Ein weiterer Zugangsweg ist das chipTAN-Verfahren. Beim chipTAN-Verfahren produziert der Kunde seine TAN selbst und zwar mit einem kleinen, kabellosen Lesegerät und der Debitkarte. Durch den Einsatz von zwei getrennten Geräten – dem chip-TAN-Lesegerät und PC, Smartphone oder Tablet – ist das Verfahren besonders sicher. Außerdem gilt die TAN nur für einen bestimmten Auftrag und das auch nur zeitlich begrenzt. Das funktioniert natürlich nur wenn man für das chip-TAN-Verfahren freigeschaltet wurde.
Das Lesegerät ist kostenpflichtig, z.Zt. 15,00€. Stellt man auch hier einen Missbrauch oder Verlust fest, ist wieder unverzüglich entweder die kontoführende Stelle oder der Sperrannahmedienst, Telefon 116116, zu informieren. Es werden alle für die betreffenden Konten ausgegebenen Karten gesperrt und der Kunde hat keinen Zugriff mehr.
Das dritte Zugangsmedium ist das MobileBanking, sprich sms-TAN-Verfahren. Dafür muss sich der Kunde sich von seinem Kreditinstitut freischalten lassen. Hierfür ist ein Mobiltelefon (Handy) sowie eine Chipkarte (SIM-Karte) des Telefonbetreibers nötig. Für das sms-TAN-Verfahren wird eine deutsche Mobilfunknummer des Netzbetreibers registriert. Auf das registrierte Handy wird dem Nutzer vom Kreditinstitut bei Bedarf eine TAN durch eine Textmeldung (SMS) in wenigen Sekunden übermittelt. Diese übermittelte sms-TAN ist nur für den Auftrag für den diese angefordert wurde. Wird auch hier Missbrauch

oder Verlust des Handys oder der SIM-Karte festgestellt, ist natürlich unverzüglich beim kontoführenden Kreditinstitut eine Sperre zu veranlassen. Zusätzlich ist das Handy auch beim Mobilbetreiber zu sperren.
Grundsätzlich ist es erlaubt, die PIN unter Verwendung einer TAN zu ändern. Die alte PIN ist dann ungültig. Sollte der Nutzer dreimal hintereinander eine falsche PIN eingegeben haben, so sperrt das Kreditinstitut den Onlinebanking Zugang zum Konto/Depot. Sperraufhebung kann erfolgen, indem er neben dem richtigen PIN eine gültige TAN eingibt. Werden allerdings dreimal hintereinander eine falsche TAN eingegeben, werden daraufhin alle nicht verbrauchten TAN der TAN-Liste für sämtliche TAN-Verfahren gesperrt. Spätestens dann sollte man sich an sein Kreditinstitut wenden.
Beim pushTAN-Verfahren erhält der Kunde eine TAN über eine spezielle App, die pushTAN-App“ direkt auf das Smartphone oder Tablett. Dazu benötigt man kein zusätzliches Gerät. Passwortschutz und kryptografische Schlüssel machen das Verfahren sicher. Auch hierbei muss der Nutzer sich natürlich von seinem Kreditinstitut freischalten lassen. Man erhält mit der Post die Zugangsdaten. Die App selber muss dann im, z.B. Google Play Store, kostenlos auf Smartphone oder Tablet heruntergeladen werden. Eine Überweisung wird z.B. im Onlinebanking vorbereitet und abgesandt, dann zur pushTAN-App wechseln, die App über Touch-ID entsperren und die angezeigten Auftragsdaten überprüfen. Danach erhält man von der App eine TAN. Sie ist nur für diese eine Überweisung gültig. Diese Zahl trägt man in das Online-Banking-Formular ein und man gibt die Überweisung frei.
Ferner haben Frau Bick und Herr Schulze uns noch auf die Möglichkeit eines ePostfaches (elektronischer Briefkasten) hingewiesen. Das ePostfach ist Teil des Online-Bankings. Dazu muss das Kreditinstitut den Kunden freischalten. Ist der Kunde freigeschaltet, hat er dort Zugriff auf alle wichtigen Unterlagen, z. B. Kontoauszüge, Kreditkartenabrechnungen, Wertpapierdokumente, Vertragsunterlagen oder Änderungen der AGB. Schnell und einfach kann der Kunde eigene Mitteilungen an seinen Berater/in schicken oder Angebote und Informationen des Kreditinstitutes erhalten. Selbstverständlich alles verschlüsselt durch Eingabe des Benutzernamens und des Online-Banking-PIN. Nun war der Zeitpunkt gekommen an dem Frau Bick und Herr Schulze uns anhand eines Demo-Kontos die praktische Anwendung von Online-Banking zeigten.
Über allem stand aber der Sicherheitsaspekt und wurde von den beiden nochmals sehr in den Vordergrund gestellt.

Ihre Tipps lauten:

- Es ist wichtig, dass man vorsichtig beim Öffnen von E-Mails sein sollte. So manche betrügerischen E-Mails sehen täuschend echt aus. Jedoch gibt es einige Punkte, die erkennen lassen, dass es eine Phishing-Email ist. Am einfachsten zu durchschauen sind z. B. E-Mails, die in fehlerhaftem Deutsch geschrieben sind. Meistens wurden sie nicht in Deutsch verfasst, sondern sind mit einem Übersetzungsdienst aus einer anderen Sprache übersetzt worden.
- Achtung wenn der Name fehlt. Das Kreditinstitut und andere Geschäftspartner sprechen den Kunden grundsätzlich mit Namen an und niemals mit "Sehr geehrter Kunde" oder "sehr geehrter Nutzer".
- Niemals auf „dringenden Handlungsbedarf“ reagieren. Wenn man via E-Mail aufgefordert wird, ganz dringend und innerhalb einer kurzen Frist zu handeln, sollte man hellhörig werden. Insbesondere, wenn diese Aufforderung mit einer Drohung verbunden ist - beispielsweise, dass sonst die EC-Karte, die Kreditkarte oder der Online-Zugang gesperrt werden.
- Ganz kriminell ist die Aufforderung, persönliche Daten sowie möglicherweise PIN oder TAN einzugeben. Banken und Online-Zahlungsdienste werden niemals den Kunden um so etwas per E-Mail bitten. PIN und TAN werden von Geldinstituten niemals telefonisch oder per E-Mail von Banken abgefragt. Dies zählt zu den wesentlichen Sicherheitsregeln von Keditinstituten.
- In immer mehr Phishing-E-Mails werden die Empfänger aufgefordert, eine Datei zu öffnen, die entweder als Anhang der E-Mail direkt beigefügt ist oder alternativ über einen Link zum Download bereitsteht. Hände weg von unerwarteten E-Mails, keinesfalls solche Dateien herunterladen und erst gar nicht öffnen. Denn in der Regel beinhaltet diese Datei einen Virus oder ein trojanisches Pferd. Angedrohten Konsequenzen wie zum Beispiel eine Kontosperrung, der Einschaltung eines

Inkassounternehmens oder anderen erfundenen Gründen sollte einen niemals dazu verleiten, eine beigefügte Datei zu öffnen!

Mit diesen wichtigen Erkenntnissen bedankten wir uns ganz herzlich bei Frau Bick und Herrn Schulze von der Sparkasse Belm und hoffen nun, dass wir gestärkt mit diesem Wissen sicher durch das Onlinebanking kommen.

Wichtige Telefon-Nummern:

Sparkassen-Kunden-Hotline	0541-324-2020
Sperrdienst 24-Stunden	116116