KONTO UND ZAHLUNGSVERKEHR
5. ONLINE BANKING

- Zielgruppe: Sekundarstufe I und II
  Klasse 8, Klasse 9, Klasse 10, Klasse 11
  Berufliche Bildung
- Fach: Fächerübergreifend
  NRW: Wirtschaft, Hauswirtschaft, Politik/ Wirtschaft
- Themenwahl: Finanzkompetenz - Zahlungsverkehr
- Materialformat: Download
- Zeitrahmen: 45 Minuten
- Erscheinungsjahr: 2017

ZIEL

Die Schülerinnen und Schüler (SuS) kennen die unterschiedlichen Möglichkeiten Online Banking zu betreiben und kennen die Gefahren, sowie die Vermeidung von Risiken.

Kernbotschaft dieser Einheit: Online Banking ist sehr praktisch und sicher, wenn man die Risiken kennt und vermeidet.

INHALTE

1. Wie funktioniert Online Banking?
2. Welche Sicherheitsmaßnahmen sind nötig?
3. Wo lauern die größten Risiken?

5.1 WIE FUNKTIONIERT ONLINE BANKING

Information

Beim Online Banking kannst du deine Bankgeschäfte von einem Computer, Smartphone oder Tablet erledigen. Hier ist es besonders wichtig gewisse Sicherheitsvorkehrungen einzuhalten. Wir gehen im Folgenden näher darauf ein.

Die Kernbotschaft: **Sicherheit ist das oberste Gesetz!**

Beim Onlinebanking habe ich einen direkten Zugriff auf den Bankrechner und zu meinen Konten.

Man kann hier zwei unterschiedliche Verfahren unterscheiden:

Browserbasiertes Internetbanking

Hier nutzt man den Zugang über die Internetseite der Bank. Diese stellt die wichtigsten Funktionen browserbasiert zur Verfügung.

Verwendung von Onlinebanking-Programmen

Mit Hilfe eines Programmes betreibt man Online Banking am heimischen PC. Hier werden zunächst offline Transaktionen vorbereitet, z. B. ein Überweisungsbeleg ausgefüllt. Danach wird erst eine Online-Verbindung zur Übertragung der gesammelten Transaktionen aufgebaut.

Umsätze und Kontoauszüge können hier dauerhaft archiviert werden.

Z. B. StarMoney, WISO, MoneyMoney (iMac), …

Verwendung von Onlinebanking-Apps

Die meisten Banken bieten eigene Apps für das Smartphone an. Mit dieser speziellen Anwendung kann man Bankgeschäfte auch unterwegs tätigen. Mit dem Smartphone ist man dann unabhängig vom heimischen PC.

5.2 WELCHE SICHERHEITSMAßNAHMEN SIND NÖTIG?

Für sicheres Onlinebanking muss nicht nur der heimische PC oder das Smartphone vor Hackerangriffen sicher sein, sondern auch das Verfahren, mit dem der Kunde einen Auftrag freigibt.

Sicher ist ein Verfahren, wenn die Transaktionsnummer (TAN) aus den…

- Überweisungsdaten erzeugt wird
- Zeitlich begrenzt ist
- Für ihre Erzeugung ein zusätzliches Gerät genutzt wird

Link: https://www.verbraucherzentrale.de/wissen/geld-versicherungen/sparen-und-anlegen/sicherheitsverfahren-beim-onlinebanking-mtan-und-chiptan-10891

🛠 Schüleraufgabe

Chancen und Risiken des Onlinebankings

Material: Meinungslinie

Mittels Kreppband wird im Raum auf dem Boden eine Linie gezogen, die eine Seite der Linie steht für „Pro ...“, die andere Seite im Raum ist dann „Contra ...“. Die Schülerinnen und Schüler haben dann die Möglichkeit, sich im Raum zu positionieren und so hinsichtlich eines Problems oder einer Frage eine Position einzunehmen („Ich bin für oder gegen etwas“). Die Pro- und Contra-Argumente des Onlinebankings können so diskutiert werden.

Mögliche Statements: Onlinebanking ist mir zu unsicher.

Onlinebanking ist besonders praktisch.

Beim Onlinebanking können schneller Fehler passieren.

Mit Onlinebanking kann man Geld sparen.

…

Die SuS die sich entsprechend aufstellen, werden nach dem Entscheidungsgrund befragt.

Zur Erzeugung der TAN gibt es verschiedene Verfahren, die im Folgenden unterschieden werden:

iTAN

Es handelt sich um eine Papierliste mit nummerierten Transaktionsnummern (meist TAN genannt). 2018 wird dieses Verfahren mit Einführung der EU-Zahlungsdienstrichtlinie PSD2 auslaufen.

Ablauf:

Die Bank gibt nach dem Zufallsprinzip vor, mit welcher TAN von der Liste der Auftrag bestätigt werden soll. Die angeforderte TAN ist dann verbraucht. Das Verfahren gilt als weniger sicher, da die TAN nicht aus den Überweisungsdaten selbst erzeugt wird.

mTAN (SMS-TAN)

Der Bank wird eine Mobilfunknummer gegeben. An diese Nummer wird dann die TAN per SMS geschickt. Die Anmeldung wird in der Regel durch eine Bestätigungs-SMS an dieses Mobilfunkgerät bestätigt.

Ablauf:

Die Überweisungsdaten werden eingegeben. Nach Eingabe fordert man eine Freigabe-SMS an. Diese wird Sekunden später aufs Handy versendet. In der SMS werden zur Sicherheit der Betrag und die Kontonummer des Empfängers wiederholt. Dies sollte man stets kontrollieren.

Für Onlinebanking auf dem Smartphone muss zur Sicherheit ein zweites Handy verwendet werden, auf welches die SMS geschickt wird.

Das Verfahren gilt als sehr sicher, da die TAN nur an registrierte Mobilfunknummern versendet wird.

ChipTAN

Die Girocard muss für das Verfahren registriert sein. Weiterhin benötigt man einen Tan-Generator. Diesen kann man bei der Bank anfordern oder ihn im Fachhandel erwerben (Kosten ca. 10-15 EUR).

Üblich ist das „Flicker-Code“ Verfahren. Hier werden die Überweisungsdaten in ein Schwarz-Weiß-Bild mit fünf Balken, ähnlich einem Strichcode, umgewandelt.

Ablauf:

Zwecks Freigabe muss man dann den TAN-Generator vor die wechselnd aufleuchtenden Balken halten. Mit den Signalen werden die Transaktionsdaten an den Generator übertragen und eine TAN erzeugt.

Hier kann man von einer sehr hohen Sicherheit sprechen, weil die TAN auf dem Generator erzeugt wird und nur mit der zugehörigen Girocard funktioniert.

Photo-TAN

Hier benötigt man ein spezielles Lesegerät (ca. 15 EUR), das Sie bei der Bank registrieren lassen müssen. Alternativ gibt es auch von einigen Banken eine Photo-Tan-App für Ihr Smartphone.

Ablauf:

Nachdem man die Überweisungsdaten eingegeben hat, wird daraus eine farbige Grafik auf dem Display erzeugt, die Sie mit dem Lesegerät oder der App scannen.

Die Tan-Generierung mit **zwei voneinander getrennten** Geräten und die Verschlüsselung der Daten bieten hohe Sicherheit.

Push-TAN

Hier wird die nötige TAN über eine spezielle App generiert. Sie erhalten die TAN also per Handy oder Tablett.

Ablauf:

Passwortgeschützte Push-TAN-App starten und die Überweisungsdaten eingeben. Danach

erhalten Sie eine Nachricht mit der TAN und den Überweisungsdaten oder Sie müssen in die Push-TAN-App wechseln, um die Daten sehen zu können.

Da die Push-TAN-App isoliert im Smartphone betrieben wird, ist es möglich, die TAN auf demselben mobilen Gerät zu empfangen, auf dem auch die Banking-App ist. Dies ist aber weniger sicher, wie die Nutzung von zwei getrennten Geräten.

Man spricht auch hier grundsätzlich von einer hohen Sicherheit, da die Banking-APP sowie die Push-Tan-APP voneinander unabhängig betrieben werden.

Genereller Hinweis:

Es sollten nur Rechner mit Firewall und Virenschutz verwendet werden.

Nutzen Sie keine öffentlichen Rechner oder öffentliches W-LAN für Online Banking.

🛠 Schüleraufgabe

Einzelarbeit mit Übungsblatt

Material*:* Arbeitsblatt 5_1 TAN-Verfahren

Das Arbeitsblatt listet die vier gängigsten TAN-Verfahren auf: iTAN, mTAN, pushTAN, chip TAN, die von den SuS richtig zugeordnet werden müssen. Ergänzend müssen einige Sätze mit Aussagen zur Sicherheit bzw. Funktion beantwortet werden.

Die SuS ordnen den Bildern das entsprechende Verfahren zu und beantworten den Lückentext.

5.3 WO LAUERN DIE GRÖSSTEN RISIKEN?

Die häufigsten Betrugsfälle werden durch sogenanntes „Phishing“ begangen.

Beim Phishing versucht man den Eindruck zu erwecken, die E-Mail käme direkt von Ihrer Bank.

Das Ziel: Klicken auf einen Link oder sogar das Öffnen einer Anlage.

Viele Virenprogramme erkennen die Gefahr, trotzdem gelingt es Kriminellen immer wieder, sich dadurch Zugangsdaten zu verschaffen.

Beispiel:

COMMERZBANK

Sehr geehrte/r [redacted]

Datum: 07.08.2016

anlässlich unserer aktuellen Sicherheitsmaßnahmen in Bezug auf unser TAN-System im Online-Banking, haben wir bei Ihrem Bankkonto einige Korrekturen vorzunehmen.

Diesbezüglich ist es nunmehr notwendig, Ihr altes TAN-Verfahren zu anullieren, bevor Ihnen ein neues, sichereres gewährt werden kann.

Bitte benutzen Sie folgendes Formular um die Änderung Ihres TAN-Systems kostenfrei durchzuführen.

Andernfalls müssen wir Ihr Konto mit **28 EUR** belasten und für die Änderung einen unserer Kundendienstmitarbeiter beauftragen, der den Prozess mit Ihnen manuell durchführen wird.

Für Ihr neues TAN-Verfahren können Sie sich bequem registrieren in dem Sie folgende Schritte durchführen:

1. Öffnen Sie Ihren E-Mail Anhang und wählen Sie das Formular aus.
2. Füllen Sie alle Daten aus und klicken Sie dann auf "Aktualisieren".
3. Sie erhalten Ihr neues TAN-Set mit weiteren Informationen i.d.R nach einer Woche per Post zugesandt.

Wir hoffen auf Ihr Verständnis und bitten etwaige Unannehmlichkeiten zu entschuldigen.

Mit freundlichen Grüßen
Ihre COMMERZBANK - **Die Bank an Ihrer Seite**

Commerzbank Aktiengesellschaft

Geschäftsräume: Kaiserplatz, 60311 Frankfurt am Main | Postanschrift: 60261 Frankfurt am Main | DE - 114 103 514 | BAK Nr. 100005

Dateianhänge

- Formular.html

Wie erkennt man eine Phishing Mail:

- Empfänger wird mit „Sehr geehrter Kunde“ angesprochen
- Aufforderung auf einen entsprechenden Link zu klicken (würde eine Bank vermeiden)
- Fehlerhaftes Deutsch

- Dringender Handlungsbedarf wird vorgegaukelt
- PIN und TAN werden von Banken NIEMALS telefonisch oder per Mail abgefragt
- Aufforderung zur Öffnung einer Datei

Schutz:

- HTML Darstellung der E-Mails deaktivieren (bei vertrauenswürdigen Absendern kann man HTML Darstellung dann aktivieren)
- Antivirenprogramme bieten Schutz vor Phishing-Mails
- Antivirenprogramm aktuell halten
- Niemals auf Phishing Mails antworten
- Viele (aktuellen) Browser warnen vor Phishing Seiten (anhand einer sogenannten Blacklist)
- Bei Verdacht: Anbieter kontaktieren (Achtung: richtige Kontaktdaten verwenden)
- Gesundes Misstrauen und aufmerksames Lesen der E-Mail
- Online Tageslimit möglichst niedrig ansetzen, um einen möglichen Schaden generell zu begrenzen.

Weiterführende Informationen:
@ https://www.verbraucherzentrale.de/wissen/geld-versicherungen/sparen-und-anlegen/phishing-onlinebanking-zieht-gauner-an-16638

Weitere Bausteine zur Vertiefung und Ergänzung des Themas:

Die Einheit „Folgen einer Kontoüberziehung“ kann mit folgenden, thematisch abgeschlossenen Bausteinen kombiniert werden:

- Baustein 1 Wahl des Girokontos
- Baustein 2 Die Kontoeröffnung
- Baustein 3 Der bargeldlose Zahlungsverkehr
- Baustein 4 Bankkarten
- Baustein 6 Folgen einer Kontoüberziehung

Hinweise zu Nutzungsrechten:

Die Handreichungen für Lehrkräfte dürfen für unterrichtliche Zwecke kopiert und genutzt werden. Dabei dürfen die Texte in ihrem Wortlaut nicht verändert werden. Damit wollen wir sicher stellen, dass fachliche und rechtliche Zusammenhänge nicht verfälscht werden.

Die Arbeitsblätter dürfen für unterrichtliche Zwecke kopiert und genutzt werden und, soweit technisch möglich, an den Bedarf der Klasse angepasst werden.

Die Bausteine 1-6 zum Thema Konto und Zahlungsverkehr sind in einem gemeinsamen Projekt aller Verbraucherzentralen erstellt worden.

www.verbraucherzentrale.de

Gefördert durch:

Bundesministerium
der Justiz und
für Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Kontakt

Verbraucherzentrale
Saarland e.V.
Haus der Beratung

Trierer Straße 22
66111 Saarbrücken

Vz-saar@vz-saar.de
Twitter: *@vzsaar*