Bargeldloser Zahlungsverkehr

Zahlen mit Karte

1. Debitkarte: Bezahlen und Geld abheben mit Karte und PIN

Mit Debitkarten wie die Girocard, wird das Konto direkt nach der Bezahlung oder Geld abheben belastet. Durch die Eingabe der PIN (Persönlichen Geheimzahl) am Terminal wird die jeweilige Transaktion sofort bestätigt und dem Geschäftskonto gutgeschrieben. Die MasterCard und die V-PAY von Visa sind Debitkarten mit denen man Europaweit Einkaufen kann.

2. ELV (Elektronisches Lastschriftverfahren) – Bezahlen mit Karte und Unterschrift

Der Kunde erteilt über den Betrag eine einmalige Einzugsermächtigung mit Unterschrift für die Belastung seines Kontos.

3. Kreditkarten

- Charge-Karte (gängige Kreditkartenart in Deutschland): Der Karteninhaber erhält monatlich eine Abrechnung über sämtliche erworbenen Waren und Dienstleistungen. Wird eine Kreditkarte bei einer Bank beantragt, wird ein sogenannter Verfügungsrahmen festgelegt. Diesen Verfügungsrahmen wird jeden Monat im Voraus gegeben - wie ein Kredit aber ohne Zinsen. Am Ende des Monats wird der Betrag komplett vom Konto abgezogen.
- **Revolving Card** (Original Credit-Card): Es besteht die Möglichkeit per Raten zu zahlen- dabei fallen Zinsen an-Bei Verzug zusätzlich Verzugszinsen.

4. Kontaktloses bezahlen

Kontaktloses Bezahlen funktioniert mit speziellen EC-Karten, Kreditkarten oder Smartphones. EC- und Kreditkarten müssen mit Mikrochips ausgestattet sein, die Zahlungsdaten speichern und an Lesegeräte an Kassen übermitteln können. Smartphones müssen mit SIM-Karten ausgestattet sein, welche die sogenannte Nahfeldkommunikation (NFC) unterstützten.

Karten zum kontaktlosen Bezahlen müssen teils mit Guthaben aufgeladen werden, teils werden Zahlungen von Konten abgebucht. Teils müssen Verbraucher beim berührungslosen Zahlen eine Geheimzahl eingeben, teils unterschreiben, teils nur die Karte auflegen. In manchen Fällen sind Zahlungen nur bis zu einem bestimmten Betrag möglich.

Was sind Vorteile und mögliche Gefahren?

Die Wirtschaft argumentiert, durch den kontaktlosen Dienst werde das Bezahlen im Geschäft schneller und bequemer. Aus Sicht von Verbraucherschützern sind die Risiken jedoch nicht zu unterschätzen: Bei Bargeld in der Geldbörse können Verbraucher - je nach Gewohnheit - leichter den Überblick behalten. Zudem besteht etwa bei Verlust oder Diebstahl der Karte oder des Handys die Gefahr, dass Fremde bis zur Sperrung einkaufen gehen können - wenn vielleicht auch nur für kleinere Beträge.

IT-Experten warnen zudem vor den Gefahren künftiger Smartphone-Viren. Bereits in der Vergangenheit gab es daneben Warnungen, dass NFC-Chips bei geringer Entfernung von wenigen Zentimetern auch durch Unbefugte ausgelesen werden könnten.

Was sind die Interessen der Wirtschaft?

Verbraucherschützern zufolge verspricht sich die Wirtschaft vom kontaktlosen Bezahlen, dass Verbraucher leichtherziger Geld ausgeben. Daneben liegt in den Geschäften weniger Geld in den Kassen. Banken könnten im Prinzip darüber nachdenken, weniger Geldautomaten aufzustellen, wenn sich der Service durchsetzt.

Quelle: https://www.n-tv.de/ratgeber/Wie-funktioniert-kontaktloses-Bezahlen-article15270871.html

Wer mit Karte bezahlt verliert schnell den Überblick seines Kontos und seiner Finanzen. Noch schwieriger ist es den Überblick zu behalten, wenn man mit Kreditkarte zahlt, da erst am Monatsende abgerechnet wird und im schlimmsten Fall nicht genug Geld auf dem Konto ist.

Tipp: Zahle öfter mit Bargeld, da Du einen genaueren Überblick behältst. Checke Deinen Kontoverlauf regelmäßig und benutze am besten keine Kreditkarte (oder nur selten).

Online Banking

1. Was ist SEPA – Single Euro Payments Area?

Die SEPA-Zahlverfahren sind europaweite Standards für Überweisungen, Lastschriften und Kartenzahlungen. Sie vereinheitlichen und vereinfachen den europäischen Zahlungsverkehr. Die Nutzung der SEPA-Zahlverfahren ist für Unternehmen, Vereine oder öffentliche Verwaltungen seit dem 1. August 2014 verbindlich.

Mit der Euro-Überweisung führen Sie einfach Überweisungen in Euro innerhalb Deutschlands, in die anderen EU-/ EWR-Staaten sowie nach Monaco, San Marino und in die Schweiz durch. Mit den SEPA-Lastschriftverfahren können Zahlungen europaweit an einen Zahlungsempfänger veranlasst werden. Die VR-BankCard (girocard), die genossenschaftlichen Kreditkarten sowie die deutschen girocard-Systeme ("electronic cash" und das Deutsche Geldautomaten-System) erfüllen die SEPA-Anforderungen.

Die IBAN: Jedes Konto in der Europäischen Union (EU) hat eine eigene "International Bank Account Number" (IBAN). Die IBAN besteht aus bis zu 34 Ziffern und Buchstaben. In Deutschland ist die IBAN 22-stellig. Sie setzt sich zusammen aus

- dem zweistelligen Ländercode DE,
- einer zweistelligen Prüfzahl,
- der achtstelligen Bankleitzahl und
- einer zehnstelligen Kontonummer.

Der BIC: Die Gesellschaft "Society for Worldwide Interbank Financial Telecommunications" (Swift) regelt den internationalen Datenaustausch zwischen Banken. Jede teilnehmende Bank erhält von ihr als internationale Bankleitzahl eine eindeutige Kennung, den "Business Identifier Code" (BIC). Dieser wurde bis 2010 auch als "Bank Identifier Code" bezeichnet. Der BIC besteht aus acht oder elf Stellen.

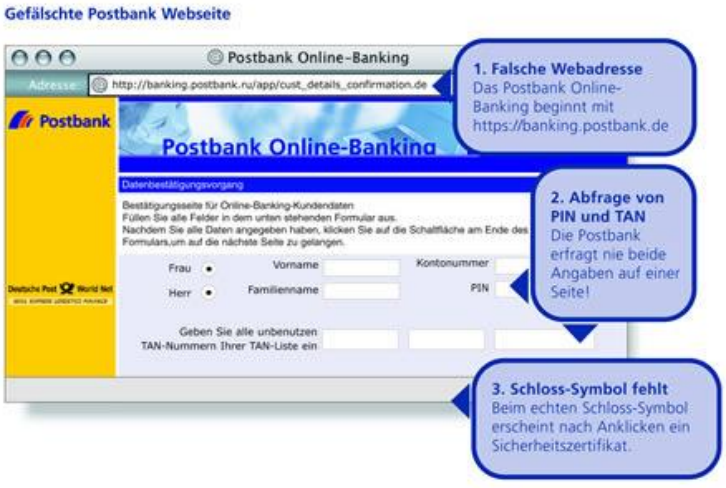
2. Gefahren und Sicherheitsrisiken

Wer Online-Banking nutzt, spart sich zwar Zeit und Mühe, weil er viele Bankgeschäfte von zu Hause aus erledigen kann – der Anwender setzt sich aber auch Sicherheitsrisiken aus. Gerade Online-Banking ist für viele Kriminelle ein beliebtes Angriffsziel, denn es lassen sich nicht selten direkt hohe Geldbeträge erbeuten.

➢ E-Mail-Phishing: Passwortdiebstahl mit manipulierten E-Mails

Beim Online-Banking weisen Kunden mit PIN beziehungsweise Passwort und TAN ihre Identität nach. Diese Daten versuchen Internet-Kriminelle daher auszuspähen und mit ihrer Hilfe an das Geld der Bankkunden zu kommen. Der Fachbegriff für dieses illegale Vorgehen heißt Phishing.

Das sogenannte E-Mail-Phishing war viele Jahre die beliebteste Methode der Internet-Kriminellen, um an Kundendaten zu gelangen. Ein Beispiel: Die Datendiebe verschicken E-Mails, die optisch wie inhaltlich offiziellen E-Mails von Bankhäusern nachempfunden sind. Darin werden die Kunden unter Angabe verschiedenster Vorwände aufgefordert, auf einen Link zu klicken, der angeblich auf die Webseite der Bank verweist. In Wahrheit führt ein Klick die Nutzer aber auf eine dem Internetauftritt der Bank nachempfundene gefälschte Webseite. Dort werden die Anwender aufgefordert, ihre Kontonummer, die PIN und einige TANs einzugeben. Mit diesen Daten können die Kriminellen dann abhängig vom verwendeten TAN-Verfahren illegal Transaktionen durchführen.



🔍Beispiel einer gefälschten Banken-Website, die auffordert alle unbenutzten Transaktionsnummern einzugeben.

- **Spear-Phishing:**

Dabei beschaffen sich Kriminelle auf illegalen Wegen persönliche Daten und E-Mail-Adressen von einer bestimmten Nutzergruppe und schreiben diese gezielt mit auf sie zugeschnittenen Nachrichten an. Es hat sich gezeigt, dass die persönliche Ansprache bei Internetnutzern zu mangelnder Vorsicht führt.

Diese Tatsache machen sich Angreifer auch zunutze, indem sie zunehmend Instant-Messaging-Dienste und soziale Netzwerke zur Verbreitung von Phishing-Nachrichten nutzen. Dabei verschicken Sie die gefälschten Nachrichten über manipulierte Zugänge im Namen von ahnungslosen Nutzern. Da das "Opfer" dem Freund vertraut, steigt die Wahrscheinlichkeit, auf solche Nachrichten hereinzufallen und Anhänge zu öffnen oder Links zu folgen.

- **Schadsoftware: Trojanische Pferde sammeln unbemerkt Daten**

Vorsicht und ein gesundes Misstrauen sind gute Mittel gegen E-Mail-Phishing-Attacken. Da Anwender sensibler für diese Bedrohung geworden sind, nutzen Kriminelle beim Erbeuten von Passwörtern zunehmend Schadprogramme. Dabei handelt es sich um sogenannte Trojanische Pferde.

Diese schleusen Angreifer auf den unterschiedlichsten Wegen auf die Rechner der Online-Banking-Anwender ein, häufig ohne dass diese die Bedrohung auf ihrem Rechner bemerken. Beim sogenannten **Man-In-The-Middle-Angriff** überwachen und manipulieren diese Schadprogramme als "Mann in der Mitte" den Datenverkehr zwischen dem Browser des Anwenders und dem Rechner der Bank. Wenn der Benutzer eine Überweisung durchführt, fängt das Schadprogramm die Auftragsdaten ab, verändert Betrag und Kontonummer des Empfängers und leitet die manipulierten Daten an die Bank weiter. Kriminelle überweisen sich auf diese Weise, also mithilfe des Schadprogrammes das Geld, das Sie eigentlich jemandem anderen zukommen lassen wollten. Sie merken davon zunächst nichts. Erst beim nächsten Blick auf einen Kontoauszug wird der Schaden sichtbar.

Bei sogenannten "**Man-In-The-Browser**"-Attacken greifen die Schadprogramme nicht in den Datenverkehr zwischen Ihrem Rechner und dem Bank-Computer ein, sondern manipulieren nur die Darstellung der Online-Banking-Webseite im Browser. Wenn Sie bei einem infizierten Rechner die Adresse der Online-Banking-Webseite eingeben, wird eine normale Verbindung hergestellt. Öffnet sich die Anmelde-Webseite des Bankportals, sorgt die Schadsoftware aber dafür, dass zwar die korrekte Webseite aufgerufen, dort aber manipulierte Inhalte angezeigt werden. Unter Vorspiegelung falscher Tatsachen wird der Nutzer zum Beispiel über eine gefälschte Eingabemaske dazu gebracht, bestimmte Daten preiszugeben – zum Beispiel TANs oder die Kreditkartendaten. Gleichzeitig deutet aber die korrekte Adresse in der Adressleiste des Browsers darauf hin, dass alles seine Richtigkeit hat. Mit derartigen Manipulationen ist es Angreifern schon gelungen, die als relativ sicher geltenden chipTAN-Verfahren auszuhebeln.

- **Mobile Banking: Unterwegs lauern Gefahren**

Es ist riskant, fremde Rechner fürs Online-Banking zu nutzen. Denn Browser speichern Daten der letzten Verbindungen in einem Zwischenspeicher ab – dem sogenannten **Cache.** Wer Bankgeschäfte etwa im Internetcafé abwickelt, riskiert, dass Kriminelle später diese Informationen im Cache auslesen. Können Sie nicht vermeiden, fremde Rechner zu nutzen, sollten Sie den Cache des Browsers in jedem Fall im Anschluss an Ihre Sitzung **löschen**.

Ein weiteres Risiko unterwegs ist der Internetzugang über öffentliche WLANs. Mithilfe eines solchen drahtlosen Netzwerkes können Sie mit Ihrem Computer ohne störende

Kabelverbindungen auf das World Wide Web und somit auch auf das Online-Banking-Angebot Ihrer Bank zugreifen. Die Funkverbindung ist allerdings nur dann sicher, wenn der Datenverkehr ausreichend verschlüsselt ist, was bei einem öffentlichen WLAN schwer zu überprüfen ist.

- **Gefahr für Smartphone-Anwender**

Grundsätzlich bestehen alle Gefahren, die Sie vom Online-Banking mit dem Heim-Computer kennen, auch beim Mobile Banking. So ist es beispielsweise auch bei Smartphones nötig, regelmäßig Updates einzuspielen, um eventuelle Sicherheitslücken zu schließen.

- niemals PIN oder TANs abspeichern.
- Unbemerkten Zugriff auf Ihr Mobiltelefon verhindern Sie unter anderem dadurch, dass Sie die Tastensperre mit Passwortschutz aktivieren.

3. Sicherheitstipps

Wenn Sie einige Grundregeln beachten, lässt sich die Sicherheit des Online-Bankings deutlich verbessern – auch wenn es niemals einen vollkommenen Schutz geben wird.

Wählen Sie Zugangsdaten sorgfältig aus und gehen Sie vorsichtig damit um.

So wie Sie am Bankschalter oder beim Geldautomaten darauf achten sollten, dass Gespräche oder die Eingabe von Kennwörtern und Zugangsdaten (PINs) nicht von Fremden mitverfolgt werden, ist auch im Internet Vertraulichkeit oberstes Gebot – das gilt im besonderen Maße für die Transaktionsnummern (TAN). Bewahren Sie die Listen mit Ihren TANs sicher auf, sodass sie nicht gestohlen oder kopiert werden können.

- Ob Sie Zugangs- und Transaktionsdaten elektronisch speichern dürfen, entnehmen Sie bitte den Bedingungen für das Online-Banking Ihrer Bank.
- Wählen Sie ein sicheres Passwort für den Zugang zum Online-Banking.
- Achten Sie beim Online-Banking darauf, dass die Kommunikation verschlüsselt erfolgt.
- Online-Banking sollte immer über das geschützte https-Protokoll erfolgen. Ob das der Fall ist, können Sie daran erkennen, dass sich der Anfang der Browserzeile verändert. Statt http:// wird dann https:// angezeigt.
- Bei der Verwendung der aktuellen Browsersoftware wird mittlerweile oftmals ein Zertifikat angezeigt, mit dem die Richtigkeit der Angaben des Servers, mit dem Sie verbunden sind, von einer unabhängigen Instanz, dem Zertifikatshersteller, bestätigt wird. Überprüfen Sie, ob der im Sicherheitszertifikat angegebene Name der Internetseite mit dem Namen Ihrer aufgerufenen Seite übereinstimmt. Dass eine Webseite zertifiziert ist, können Sie daran erkennen, dass nach der URL ein kleines Schloss-Symbol angezeigt wird. Bei einem Klick auf das Schloss-Symbol erhalten Sie mehr Informationen über das Zertifikat und ob die Webseite tatsächlich die ist, für die sie sich ausgibt.
  Wenn ein Anbieter sich nicht mit einem gültigen Zertifikat als tatsächlicher Besitzer der Adresse ausweisen kann, erhalten Sie von Ihrem Browser eine Warnmeldung. In diesem Fall sollten Sie die Transaktion sofort abbrechen und Ihre Bank informieren.
- W-LAN verschlüsseln.
- **Prüfen Sie die Echtheit der Bank-Webseite:** Achten Sie auf Phishing also Fälschungen
- **Betreiben Sie Online-Banking – soweit möglich – nur von eigenen Geräten aus** (Cache löschen)

- Vereinbaren Sie mit Ihrer Bank ein Limit für tägliche Geldbewegungen beim Online-Banking.
- **Überprüfen Sie regelmäßig Ihre Kontobewegungen** (gedruckte Versionen sind korrekt)
- **Seien Sie sparsam bei der Weitergabe Ihrer Bankverbindung.**
- **Sperren Sie Ihren Online-Banking-Zugang, wenn Ihnen etwas verdächtig vorkommt.**

4. Was tun im Ernstfall?

Woran erkennen Sie, dass Sie Opfer eines Phishing-Angriffs geworden sind? Es gibt eine Reihe von Anzeichen, bei deren Auftreten Sie misstrauisch werden sollten:

- Nach der Eingabe von Anmeldename oder Legitimations-ID und -PIN zur Anmeldung werden Sie zum Beispiel auf einer manipulierten Folgeseite zur Eingabe von mehreren unbenutzten TANs und den dazugehörigen laufenden Nummern aufgefordert. Achten Sie bitte grundsätzlich bei der TAN-Eingabe darauf, dass diese in Verbindung zu Ihrem Auftrag (zum Beispiel einer Überweisung) steht.
- Während des Online-Banking-Vorgangs öffnet sich ein neues Browser-Fenster. Sie werden aufgefordert, Ihre Bankleitzahl, PIN und/oder eine oder mehrere TANs einzugeben.
- Sie werden während oder nach Abschluss einer Transaktion aufgefordert, eine oder mehrere TANs einzugeben. Oft erscheint die Meldung, dass die vorher eingegebene TAN bereits verbraucht oder falsch sei.
- Ihre gesicherte Verbindung zum Online-Banking wird nach Eingabe von PIN und TAN unterbrochen.
- Ihr Internet-Browser wird ohne ersichtlichen Grund geschlossen. Eventuell wird eine entsprechende Fehlermeldung angezeigt.
- Nach dem Abschluss einer Transaktion durch Eingabe einer TAN zeigt Ihr Internet-Browser die Fehlermeldung an, dass das Online-Banking nicht mehr erreichbar ist. Die Meldung wird Ihnen wiederholt angezeigt, wenn Sie zu einem späteren Zeitpunkt das Online-Banking starten möchten.

Wenn eine der oben genannten Auffälligkeiten auftritt oder Sie aus einem anderen Grund den Eindruck oder den Verdacht haben, dass etwas nicht stimmt, sollten Sie sofort aktiv werden:

1. Sperren Sie unverzüglich Ihr Bankkonto und Ihren Zugang zum Online-Banking. Am schnellsten geht das, indem Sie zum Beispiel die Anmeldemaske zum Online-Banking aufrufen und dreimal hintereinander die falsche PIN eingeben. Oder rufen Sie den zentralen Sperr-Notruf 116 116 (aus dem Ausland +49 116 116) an und lassen Sie Ihren Zugang telefonisch sperren.
2. Danach wenden Sie sich sofort an Ihre Bank und melden die Auffälligkeiten. Gegebenenfalls besteht die Möglichkeit, Kontobewegungen rückgängig zu machen.
3. Prüfen Sie umgehend die Kontoumsätze anhand des Papierauszuges.
4. Sollten Sie Opfer eines Phishing-Angriffs mittels eines Trojaners geworden sein, müssen Sie Ihren PC fachgerecht von der Schadsoftware befreien.