Bei Verdacht: Kontaktieren Sie uns unter der kostenfreien Rufnummer 0800 1008906 – rund um die Uhr. Oder senden Sie eine E-Mail an missbrauch@postbank.de

Deutsche Postbank AG
Zentrale
Marken und Marketingkommunikation
Bonn

100 % chlorfrei gebleichter
Zellstoff
678 142 024
Stand: Januar 2015

Postbank
Eine Bank fürs Leben.

Wichtige Informationen zur Betrugsprävention

Betrugsmethoden bei Geldgeschäften

In Kooperation mit

Wir wollen, dass Sie sicher leben. Ihre Polizei
www.polizei-beratung.de

Postbank
Eine Bank fürs Leben.

Betrügern keine Chance

Die Methoden der Betrüger bei Geldgeschäften werden immer raffinierter und für die potenziellen Opfer schwerer zu erkennen.

In Kooperation mit der Polizei möchten wir Sie daher auf den folgenden Seiten für die geläufigsten Betrugsmethoden sensibilisieren und Ihnen zeigen, wie Sie sich am besten schützen können. Erfahren Sie hier,

- was Sie beim Transfer von Bargeld misstrauisch stimmen sollte und wie Sie sich vor bösen Überraschungen schützen können
- worauf Sie bei Abhebungen am Geldautomaten achten sollten
- mit welchen Methoden Betrüger im Internet versuchen, an Ihr Geld zu kommen

Zu Ihrer Sicherheit: Überdurchschnittlich gute Ergebnisse in den Testfeldern Sicherheit und Kundenorientierung bringen das Postbank Online-Banking auf Platz 1 von insgesamt 36 getesteten Banken. FOCUS-MONEY hat für diese Studie das renommierte Institut für Management und Wirtschaftsforschung (IMWF) beauftragt.

In Kooperation mit

Wir wollen, dass Sie sicher leben. Ihre Polizei

www.polizei-beratung.de

Sicherer Geldtransfer

Sendungen von Bargeld müssen maximal sicher sein. Deswegen hat sich die Postbank mit Western Union einen zuverlässigen, renommierten Partner und Experten gewählt.

Geldtransfers werden in Deutschland vor allem von Menschen mit fremder Herkunft genutzt, die ihre Familien im Heimatland finanziell unterstützen. Der Service ist auch praktisch, wenn auf einer Reise nach Verlust des Portemonnaies dringend Geld benötigt wird, oder für ein spontanes Geldgeschenk. Hier bieten die Geldtransfers von Western Union schnelle Hilfe, da der Kunde an nahezu 500.000* Agenturen in über 200 Ländern Bargeld in Empfang nehmen kann.

* Anzahl der Standorte: Stand 01.10.2014.

Für den Geldtransfer brauchen Kunden weder ein Girokonto, noch müssen sie sich vorher anmelden. Auftraggeber füllen lediglich ein Formular aus, weisen sich mit einem gültigen Ausweisdokument aus und übergeben den Sendebetrag dem Filialmitarbeiter. Den Empfängern steht das Geld wenige Minuten später zur Verfügung.

Grundsätzlich gilt: Wer bares Geld transferiert, sollte immer ganz sicher sein, wer es bekommt. Western Union bietet eine kostenlose Service-Nummer, die Sie bei Betrugsverdacht bitte anrufen: 0800 4044014.

Klarer Fall von Misstrauen

Ihr bester Schutz ist Vorsicht. Bewahren Sie persönliche Daten und Nummern sorgfältig auf, lassen Sie sich z. B. nicht zu einem Kauf drängen und pflegen Sie stets ein gewisses Maß an Misstrauen.

Hier einige Beispiele für typische Betrugsmaschen:

- **Verführerische Angebote –** Geldtransfers zur Bezahlung von Wohnungsmiete, Fahrzeugen oder Online-Käufen sollten nie getätigt werden; auch wenn das damit verbundene Angebot sehr verführerisch klingt. Besonders bei ungewöhnlichen Angeboten sollte man nie in Vorleistung treten, ohne die dafür versprochene Leistung erhalten zu haben. Erst wenn man sich davon überzeugt hat, dass die Wohnung und das Auto tatsächlich existieren und das gekaufte Produkt einwandfrei ist, sollte man Geld überweisen.

- **Vorsicht bei Schecks –** bei dieser Betrugsmasche schließt der Verkäufer (Opfer) mit dem Käufer (Betrüger) ein Geschäft ab. Der Verkäufer erhält zur Bezahlung einen Scheck, durchaus von einer bekannten Bank ausgestellt. Die Summe übersteigt den vereinbarten Preis um ein Vielfaches. Der Käufer behauptet, dass ein Missverständnis vorliege, und drängt den Verkäufer, den Scheck einzulösen, den Differenzbetrag abzuheben und per Geldtransfer zurückzuschicken. Dass der Scheck gefälscht ist, stellt sich oft erst nach dem Geldtransfer heraus. Damit ist der Verkäufer dreifach betrogen: um die Ware, den Verkaufspreis und den „Differenzbetrag".

- **Gefälschte Gewinnbenachrichtigungen –** die Opfer erhalten Telefonanrufe oder E-Mails, in denen behauptet wird, sie hätten beispielsweise Geld oder ein Auto gewonnen. Der Gewinn stehe angeblich bereit, es müsse nur eine Gebühr für Zoll oder Transport bezahlt werden, damit der Preis übergeben werden könne. Den Gewinn erhält das Opfer trotz Bezahlung nicht, und eine Chance, sein Geld zurückzuerhalten, besteht kaum.

- **Identitätsdiebstahl im Internet –** Kriminelle greifen Zugangsdaten ab, beispielsweise zu sozialen Netzwerken oder E-Mail-Postfächern. Freunde und Familienmitglieder erhalten daraufhin gefälschte Nachrichten, dass sich die Person in Not befinde und dringend Geld benötige. Treten Freunde und Familie dann per Internet mit der Person in Kontakt, wird diese Korrespondenz umgeleitet, sodass diese Person nichts erfährt. Hier ist es erforderlich, auf direktem Weg mit dem vermeintlich in Not geratenen Freund oder Verwandten zu sprechen, um die Situation zu klären.

- **Romance- oder Love-Scamming –** Tatort: soziale Netzwerke und Online-Partnerbörsen. Auf sehr perfide Weise werden Kontakte geknüpft und sehr taktisch gepflegt – so intensiv, dass eine Liebesbeziehung entsteht, damit einher emotionale Abhängigkeit. Sobald dieses Teilziel erreicht ist, wird eine finanzielle Notsituation geschildert, z. B. angeblicher Raub auf einer Geschäftsreise in Afrika oder eine plötzlich dringende Operation eines Kindes. Nach der Geldübergabe meldet sich der Betrüger nie wieder.

Denken Sie daran, dass Geldtransfers innerhalb kurzer Zeit ausgezahlt werden. Nach der Auszahlung wird der Betrag im Betrugsfall nicht erstattet.

Sicher Bargeld abheben

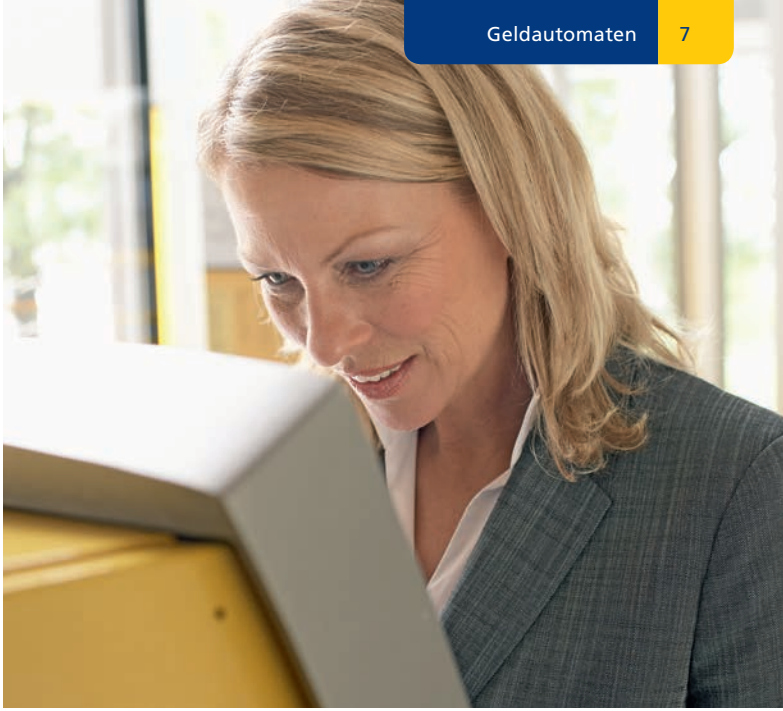
Geldautomaten geraten immer wieder in den Fokus von Betrügern. Ein wenig Vorsicht und erhöhte Aufmerksamkeit schützen Sie zuverlässig.

Aktuelle Betrugsmaschen am Geldautomaten

Mit Cash-Trapping (Geldfallen) haben Betrüger es nicht nur in Deutschland, sondern europaweit verstärkt darauf abgesehen, Bargeld direkt beim Abhebevorgang am Geldautomaten abzufangen. Dabei wird über dem Geldausgabefach eine täuschend echte Blende angebracht, die verhindert, dass das Bargeld ausgegeben wird – die Geldscheine bleiben buchstäblich im Ausgabefach kleben. Die meisten Kunden vermuten einen technischen Defekt, obwohl kein Störungshinweis auf dem Monitor des Geldautomaten erscheint. Nachdem sich die Kunden vom Geldautomaten entfernt haben, entnehmen die in der Nähe wartenden Täter die Blende und das Bargeld. Eine weitere Variante ist, dass bei Eingabe des Auszahlungsbetrags das Opfer überraschend abgelenkt wird. Die Täter wählen vom Kunden unbemerkt den Höchstauszahlungsbetrag und entnehmen ungesehen das Geld.

Bitte beachten Sie:

- Überprüfen Sie den Geldautomaten und seine Umgebung. Bemerken Sie etwas Ungewöhnliches? Verschieben Sie die Bargeldauszahlung auf einen anderen Zeitpunkt, wenn Ihnen Personen verdächtig vorkommen!
- Behalten Sie den Karten- und Geldausgabeschacht immer im Blick!
- Zählen Sie die ausgegebenen Geldscheine unbedingt sofort nach.
- Kontrollieren Sie regelmäßig Ihre Kontoauszüge.



Skimming

Skimming ist die Methode, illegal Daten des Magnetstreifens von Karten am Geldautomaten auszulesen und die dazugehörige Geheimzahl auszuspähen. Dies geschieht durch ein unscheinbares Gerät, das am Schacht angeklebt wird, da, wo die Karte eingeführt wird. Zusätzlich wird eine Kamera in der Umgebung des Geldautomaten platziert, um die Geheimzahl-Eingabe aufzuzeichnen. Solche Aufsätze können sich auch auf Lesegeräten, die den Zugang zum 24-Stunden-Bereich ermöglichen, befinden!

Bitte beachten Sie:

- Decken Sie Ihre PIN-Eingabe immer mit der freien Hand ab.
- Manche Geldautomaten haben ein sogenanntes „Froschmaul". Dies ist ein transparentgrüner Aufsatz oberhalb des Kartenschlitzes mit einem eingravierten Schlosssymbol. Es erschwert Kriminellen das Anbringen von Skimming-Geräten.
- Wenn Ihnen etwas verdächtig erscheint, rufen Sie uns umgehend unter der kostenlosen Nummer 0800 0332565 an.

Internet – das Netz mit den vielen Maschen

Schnell, unkompliziert, mal eben nebenbei surfen im Internet – heute selbstverständlich. Aber die Beiläufigkeit, mit der das Medium genutzt wird, birgt die Gefahr, Stolperfallen zu übersehen. Besonders bei Käufen.

Wir schärfen Ihren Blick für Dinge, die auf Betrug hinweisen. Ob im Rahmen des Online-Bankings, wo es direkt an Ihr Geld geht, oder mittels anderer Online-Zugänge, die mittelbar dasselbe Ziel anvisieren.

Geläufigste Betrugsmethoden

Phishing
Gefälschte Mails, scheinbar von der Postbank, fordern Sie auf, zu einer ebenfalls gefälschten Website zu linken. Dort wird verlangt, Ihre Zugangsdaten wie Kontonummer oder PIN zum Online-Banking in vorgefertigte Felder einzutragen, um beispielsweise an einem Gewinnspiel teilzunehmen. Die Zugangsdaten werden von den Betreibern der Betrugsseite registriert und zeitnah missbraucht.

Social Engineering
Darunter versteht man einen Angriff, der nicht auf einen Computer gerichtet ist, sondern auf dessen Benutzer, mit dem Ziel, Login-Daten oder Passwörter auszuspähen. Den Kontakt stellen die Angreifer z.B. per Mail oder Telefon her.

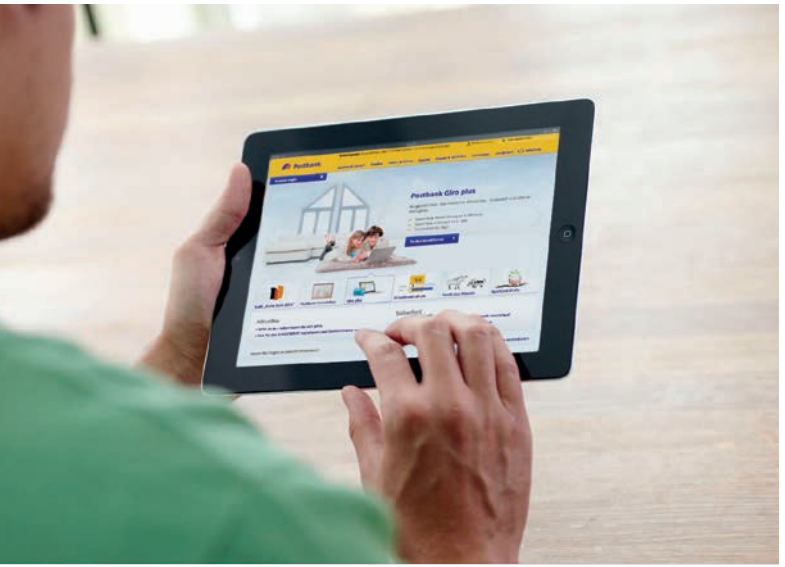
Trojaner
Es gibt kleine Programme, die scheinbar ganz nützlich sind und deswegen auf den Rechner geladen werden. Einmal installiert, werden sie jedoch gefährlich: Sie leiten den Nutzer unbemerkt auf gefälschte Webseiten. Dort werden dann Daten zum Online-Banking ausspioniert.

Bitte beachten Sie:

- Die Postbank hat klar erkennbare Internetadressen.
- Die Sprache der Postbank ist verständlich und fehlerfrei.
- Gewinnspiele sind bei der Postbank möglich, es werden dafür aber niemals persönliche Zugangsdaten erfragt.
- Achten Sie auf die Echtheit der E-Mail durch ihre Signatur, Sie finden sie mit einem Klick auf das Schlosssymbol am Seitenrand einer jeden E-Mail der Postbank, siehe auch (www.postbank.de/email-signatur).
- Ignorieren Sie E-Mails ohne Signatur, die angeblich von der Postbank stammen, grundsätzlich! Löschen Sie diese oder senden Sie sie an missbrauch@postbank.de
- Die Postbank wird Sie niemals darum bitten, eine Testüberweisung durchzuführen, einen „fälschlicherweise" zugestellten Betrag zurückzuüberweisen oder persönliche Daten wie z. B. das Geburtsdatum oder die Personalausweisnummer online abfragen. Im Zweifel sollten Sie immer anrufen und die Rechtmäßigkeit hinterfragen.

Bitte beachten Sie:

- Software (Browser, Apps, Freeware etc.) nur von vertrauenswürdigen Quellen beziehen
- Dateianhänge von E-Mails, deren Absender Ihnen nicht vertrauenswürdig erscheinen, ungelesen löschen
- sensible Daten (Kennwörter, PIN etc.) nie auf der Festplatte speichern
- täglich Virenscanner aktualisieren



Bei Verdacht auf Online-Betrug rufen Sie uns kostenfrei an unter 0800 1008906! Aktuelle Informationen finden Sie unter www.postbank.de/sicherheit

TAN-Missbrauch

Die Masche: Sie werden per E-Mail aufgefordert, Zugangsdaten zu überprüfen. Dabei sollen die Empfänger eine Testüberweisung durchführen, angeblich würde kein Betrag gebucht. In Wirklichkeit wird aber der Betrag, der auf dem Endgerät des Sicherheitsverfahrens (Handy bei mobile TAN, chipTAN Generator, BestSign Gerät oder App) angezeigt wird, tatsächlich überwiesen. Bestätigt das Opfer die angezeigte Transaktion, so wird diese auch ausgeführt.

Bitte beachten Sie:

- Die Postbank wird Sie nie per Mail auffordern, eine Zahlung auszulösen, auch nicht zu Testzwecken, eine PIN zu ändern oder eine TAN ohne Prüfung der Auftragsdaten einzugeben.
- Prüfen Sie, ob die aufgerufene Seite mit „https“ beginnt und ob sie ein gültiges Sicherheits-Zertifikat hat (erkennbar durch Klick auf das Schloss).
- Überprüfen Sie stets die Daten, die Ihr Endgerät des jeweiligen Sicherheitsverfahrens anzeigt, ob die Informationen mit Ihren Daten übereinstimmen.
- Brechen Sie grundsätzlich die Transaktion sofort ab, wenn Ihnen etwas komisch vorkommt.