Die sichere Nutzung Ihrer ING Corporate Card

Einführung

Mit Ihrer ING Corporate Card können Sie unter anderem Hotelübernachtungen, Kongresse, Flugtickets, Restaurants und Taxis bezahlen. Aber die Corporate Card bietet noch vieles mehr.

Denken Sie beispielsweise an Reisebüros, die sich bei der Buchung für die Annehmlichkeiten der Corporate Card entschieden haben. Immer mehr Menschen nutzen die Corporate Card wegen ihrer Bequemlichkeit und Sicherheit bei (geschäftlichen) Zahlungen.

Sie möchten natürlich gern sicher sein, dass Ihre Zahlungen gut abgewickelt werden. Dieses Dokument bietet Ihnen die Informationen dazu. ING setzt alles daran, dass der Zahlungsvorgang sicher ist und dies auch bleibt. Aber das können wir nicht ohne Sie tun. Wenn Sie sich an die grundlegenden Regeln halten, dann haben Kriminelle kaum eine Chance.

Diese grundlegenden Regeln erläutern wir Ihnen in dieser Broschüre. Wir geben Ihnen Tipps, wie Sie sicher zahlen und Betrug erkennen können, und erklären Ihnen, was wir als ING tun, damit die Nutzung Ihrer Corporate Card möglichst sicher bleibt. Weiter hinten in dieser Broschüre finden Sie ein Glossar, in dem die hier vorkommenden (Internet)Begriffe erklärt werden.

Praktisch und kostenlos

Nutzen Sie die ING Commercial Card App und nutzen Sie das ING Commercial Card Portal. Hiermit behalten Sie den Überblick über Ihre Abbuchungen, Ihre Kontoauszüge, Ihre Gesamtausgaben, Ihren Saldo und Ihr verbleibendes Limit. Die ING Commercial Card App finden Sie im Apple App Store sowie in Google Play (Android).
Um die App zu finden, geben Sie Folgendes ein: ING Commercial Card App
Das ING Commercial Card Portal finden Sie unter: www.ingcommercialcard.com

Betrug direkt melden

Sind Sie das Opfer eines Betrugs mit Ihrer Corporate Card geworden? Melden Sie uns das bitte direkt. Dann können wir Ihnen und anderen Kunden helfen - jetzt und in Zukunft. Wir sind 24 Stunden pro Tag, sieben Tage die Woche für Sie erreichbar, auch vom Ausland aus und ebenfalls über unsere Nummern zum Lokaltarif. Diese finden Sie am Ende der Broschüre.

Inhalt

1. Die fünf grundlegenden Regeln für sicheren Zahlungsverkehr

Wir haben für Sie die einheitlichen Sicherheitsregeln von Banken in den Niederlanden in fünf grundlegende Regeln für die Nutzung Ihrer Corporate Card übersetzt. Sie können sie sich auf diese Weise leicht merken.

Grundlegende Regel Nr. 1: Schützen Sie Ihre Codes/Passwörter

Ihren Hausschlüssel geben Sie nicht einfach einem willkürlichen Passanten in die Hand. Machen Sie das also auch nicht mit Ihren Sicherheitscodes/Passwörtern. Schützen Sie diese bitte gut.

- **Merken Sie sich Ihre Codes/Passwörter**
  Wählen Sie für Sicherheitscodes/Passwörter nicht ein Geburtsjahr, den Namen eines Familienmitglieds oder einen anderen Code, der einfach zu erraten ist. Haben Sie Angst, Ihre Codes/Passwörter zu vergessen? Notieren Sie diese dann so, dass andere sie nicht entziffern können oder versuchen Sie, sich eine Eselsbrücke auszudenken. So ist ein aus Großbuchstaben und Ziffern bestehender Satz eine starke Kombination, die man sich einfach merken kann. Beispielsweise: ‚Lieber U2 als die 6. von Beethoven!' Wenn es nicht möglich ist, den ganzen Satz zu verwenden, können Sie die ersten Buchstaben eines jeden Worts nehmen: 'LU2dd6evB!'

- Eine Möglichkeit, sich das Passwort Ihrer Corporate Card einzuprägen, wäre für jede Ziffer des Passworts ein Wort zu wählen, wobei die Anzahl der Buchstaben der Zahl entspricht. Aus diesen vier Worten konstruieren Sie danach einen Satz. Angenommen Ihr Passwort lautet: 9246. Sie können dann beispielsweise den Satz konstruieren: „Erinnerst (9) du (2) dich (4) Johann (6)."

- **Lassen Sie niemand zuschauen**
  Sorgen Sie dafür, dass niemand einsehen kann, wie Sie Ihre Codes/Passwörter eingeben. Das können Sie vermeiden, indem Sie beispielsweise das Tastenfeld mit Ihrem Körper oder mit Ihrer freien Hand abschirmen.

- **Geben Sie niemals einer anderen Person Ihre Codes/Passwörter**
  Werden Sie von jemandem nach Ihren Sicherheitscodes oder Passwörtern gefragt, beispielsweise für das Commercial Card Portal? Bitte geben Sie diese niemals heraus. Ihre Codes/Passwörter sind rein persönlich. Verraten Sie sie somit niemandem und merken Sie sich, dass ING-Mitarbeiter Sie nie nach Ihren Sicherheitscodes/Passwörtern fragen: nicht am Schalter, nicht am Telefon, nicht per E-Mail, nicht über eine andere Website oder APP als die van ING und auch nicht auf eine andere Weise.

Grundlegende Regel Nr. 2: Passen Sie gut auf Ihre Corporate Card auf

Ihr Portemonnaie lassen Sie nicht herumliegen. Machen Sie das also auch nicht mit Ihrer Corporate Card. Daher - passen Sie gut auf sie auf.

- **Gehen Sie sorgfältig mit Ihrer Corporate Card um.**
  Ihre Corporate Card ist rein persönlich. Verleihen Sie sie somit nicht. Lassen Sie Ihre Corporate Card nirgendwo liegen und verwahren Sie sie nach Benutzung direkt am selben sicheren Ort. Sorgen Sie dafür, dass niemand Ihre Corporate Card unbemerkt mitnehmen kann.

  Geben Sie Ihre Corporate Card lieber nicht einem Kellner mit, sondern gehen Sie besser selbst mit zum Zahlungsterminal. Ist es doch erforderlich, dass Sie Ihre Corporate Card aus der Hand geben? Überprüfen Sie dann, dass Sie Ihre eigene Karte zurückbekommen.

Kontrollieren Sie mindestens einmal pro Tag, ob Sie noch im Besitz Ihrer Corporate Card sind. Dies stellt eine Verpflichtung dar, die auch in unseren Geschäftsbedingungen steht.

- **Lassen Sie sich nicht ablenken.**
  Lassen Sie sich bei der Benutzung Ihrer Corporate Card nicht ablenken. Wenn Sie kurz unaufmerksam sind, kann Ihre Corporate Card zum Beispiel leicht mit einer Kreditkarte derselben Farbe vertauscht werden. Darum nennen wir das den Tauschtrick. Folgen Sie Ihrem Gefühl, wenn Sie vermuten, dass die Benutzung Ihrer Kreditkarte nicht sicher ist, und belassen Sie Ihre Corporate Card an ihrem sicheren Ort.

- **Kontrollieren Sie regelmäßig, dass Sie noch im Besitz Ihrer Corporate Card sind**
  Werden Sie auf der Straße von einer x-beliebigen Person angesprochen? Ist jemand mit Ihnen zusammengestoßen? Kontrollieren Sie danach immer, ob Sie noch im Besitz Ihrer Corporate Card sind. Bekommen Sie Ihre Karte nicht zurück, nachdem Sie sie zum Bezahlen benutzt haben? Nehmen Sie dann direkt Kontakt zu uns auf (24 Stunden pro Tag, sieben Tage die Woche) unter der Nummer: +31 (0)10 428 95 81 oder über eine unserer Nummern zum Lokaltarif (diese finden Sie im hinteren Teil dieser Broschüre) .

Grundlegende Regel Nr. 3: Sichern Sie Ihre Geräte

Ihre Haustür schließen Sie ab. Machen Sie das gleiche mit den Geräten, die Sie zur Durchführung von Internetabbuchungen mit Ihrer Corporate Card benutzen, wie Ihrem Telefon, Tablet, Desktop-Computer und Laptop. Daher - sichern Sie diese gut. Dann bekommen Kriminelle keine Chance, Schadsoftware zu installieren und beispielsweise mittels eines ‚Trojaners' personenbezogene Daten, wie Ihre Corporate-Card-Daten, ausfindig zu machen.

- **Installieren Sie nur legale und bekannte Software**
  Sorgen Sie dafür, dass Ihr Telefon so eingestellt ist, dass Apps unbekannter Herkunft nicht akzeptiert werden. Daher - nehmen Sie auf Ihrem Telefon kein ‚Root' oder ‚Jailbreak' vor und laden Sie nur Apps aus offiziellen App Stores herunter. Installieren Sie nur legale Software, deren Herkunft Sie kontrolliert haben. Diese Kontrolle können Sie durchführen, indem Sie sich auf der offiziellen Website des Anbieters informieren. Wird Ihnen ein unbekanntes Softwareprogramm angeboten? Laden Sie das Programm dann nicht direkt herunter, sondern kontrollieren Sie es erst mit Hilfe eines Virusscanners.

- **Benutzen Sie die neueste Version der App und Ihres Betriebssystems**
  Sowohl die Commercial Card app als auch das Betriebssystem von Ihrem Telefon, Tablet und Computer werden regelmäßig mit weiterer und besserer Sicherheitstechnologie ausgestattet. Daher - nehmen Sie regelmäßig eine Aktualisierung vor. Stellen Sie vorzugsweise automatische Updates (Aktualisierungen) ein.

- **Versehen Sie Ihr Gerät mit einem Zugangscode**
  Mit einem Zugangscode vermeiden Sie, dass andere Personen leicht Zugang zu Ihren personenbezogenen Daten bekommen. Denken Sie dabei nicht nur an Ihre Corporate Card-Daten, sondern auch an Ihre Kontakte, Mitteilungen und Fotos.

- **Benutzen Sie Virusscanner, Firewall und Anti-Spyware.**
  Benutzen Sie für Ihre Internetzahlungen mit Ihrer Corporate Card nur einen Desktop-Computer oder Laptop, der mit Virusscanner, Firewall und Anti-Spyware ausgestattet ist. Viren und unerwünschte Programme haben dann eine geringere Chance. Auch für Telefone und Tablets gibt es bereits Virusscanner, die zusätzlichen Schutz bieten.

- **Sichern Sie Ihre drahtlose Internetverbindung (WiFi)**
  Ohne eine gesicherte Internetverbindung können Sie mit Ihrer Corporate Card keine sicheren Internetabbuchungen durchführen. Sichern Sie deshalb Ihre eigene Internetverbindung mit einem Passwort. Dabei kann Ihnen Ihr Internetprovider helfen. Nutzen Sie außerhalb Ihrer eigenen vier Wände ein öffentliches WiFi-Netz? Führen Sie dann besser keine Internetabbuchungen mit Ihrer Corporate Card durch.

Grundlegende Regel Nr. 4: Kontrollieren Sie Ihre Zahlungen und Abbuchungen

Es ist immer gut, im Voraus sorgfältig zu bedenken, was Sie genau bezahlen. Und überprüfen Sie auch regelmäßig, was danach abgebucht wird. Dies ist anhand das ING Commercial Card Portal oder mit der ING Commercial Card App möglich. Die ING Commercial Card App zeigt unter anderem Ihre Abbuchungen in Echtzeit.

- **Merken Sie sich, was Sie bezahlen**
  Kontrollieren Sie, ob der von Ihnen zu zahlende Betrag korrekt auf dem Display (auf der Anzeige) erscheint oder - wenn Sie im Ausland noch auf dem Bon unterschreiben müssen - ob auf dem Bon der korrekte Betrag steht. Heben Sie die Kopie des Bons für Ihre eigene Buchhaltung auf. Damit haben Sie immer einen Beweis in Händen, wenn der später auf Ihrem Corporate Card-Kontoauszug erscheinende Betrag nicht korrekt ist.

  Sorgen Sie dafür, dass der in der Fremdwährung aufgeführte Betrag Sie im Nachhinein nicht überrascht, wenn er in den Betrag umgerechnet wird, der Ihnen auf Ihrer Corporate Card in Rechnung gestellt wird.

- **Halten Sie die richtige Reihenfolge ein**
  Tragen Sie bei einem Internetkauf erst Ihre Daten wie Kreditkartennummer, Ablaufdatum und Sicherheitscodes ein, wenn Sie sich Ihres Ankaufs sicher sind.

- **Online sehen Sie sich Ihre Abbuchungen an**
  Kontrollieren Sie Ihre Abbuchungen mindestens einmal alle vierzehn Tage. Dann können Sie beurteilen, ob Abbuchungen berechtigt sind oder nicht, und uns bei Missbrauch direkt informieren.

- **Melden Sie einen Schaden rechtzeitig**
  Wenn ein Schaden dadurch entsteht, dass es Ihnen eine gewisse Zeitlang unmöglich war, Ihre Corporate-Card-Auszüge zu kontrollieren, können wir Sie bitten, dies nachzuweisen. Ein Schaden, der später als dreißig (30) Tage nach dem Datum Ihres Kontoauszugs gemeldet wird, wird im Prinzip nicht erstattet.

Grundlegende Regel Nr. 5: Rufen Sie, im Zweifelsfalle, ING an

Sollten Sie sicher sein oder vermuten, dass Sie einem Betrug zum Opfer gefallen sind, dann informieren Sie uns bitte direkt darüber. Indem Sie Kontakt mit uns aufnehmen, können wir direkt eingreifen und einen eventuellen weiteren Schaden vermeiden. Wir lassen beispielsweise betrügerische Websites sperren, so dass nicht noch weitere Kunden Opfer des Betrugs werden.

- **Direkter Anruf**
  Wenn Sie einen Betrug vermuten, können Sie uns direkt anrufen. Dies gilt auch, wenn Ihre Corporate Card, ING Commercial Card App oder ING Commercial Card Portal User-ID blockiert sind. Oder wenn Sie eine Ihnen suspekte E-Mail erhalten haben und wenn jemand versucht hat, Ihnen Ihre Corporate-Daten zu entwenden.

- **Sorgen Sie dafür, dass wir Sie auch erreichen können**
  Im Falle von suspekten Abbuchungen möchten wir Sie gern schnell erreichen können - telefonisch oder über eine SMS-Mitteilung. Daher möchten wir Sie bitten, unserem Kundendienst Ihre Handynummer zu geben. Das können Sie über die +31 (0)10 428 9581 oder über unsere Nummern zum Lokaltarif, (die Sie im hinteren Teil der Broschüre finden), tun.

2. Erkennen Sie einen Betrug

Trotz aller Sicherungsmaßnahmen und der sorgfältigen Nutzung durch Sie selbst besteht die Gefahr des Missbrauchs Ihrer Corporate Card. Die nachstehenden Informationen sollen Sie bei der Erkennung der verschiedenen Missbrauchsversuche unterstützen.

Betrug anhand Ihrer Corporate Card

- **Skimming**
  Eine bekannte Betrugsform nennt man Skimming, wobei die auf dem Magnetstreifen stehenden Kreditkartendaten kopiert werden. In den vergangenen Jahren sind verschiedene Maßnahmen gegen das Skimming ergriffen worden. Dadurch kommt diese Form des Betrugs immer seltener vor.

- **Diebstahl, Tauschtricks und Ablenkungsmanöver**
  Noch immer kommt es vor, dass Corporate Cards vertauscht oder gestohlen werden und Sicherheitscodes während ihrer Eingabe ausspioniert werden. Es werden auch Menschen am Geldautomaten abgelenkt, und dann machen sich die Diebe mit dem aus dem Geldautomaten gezogenen Geld aus dem Staub. Ein Beispiel hierfür ist der Zehner-Trick. Sie werden mittels eines auf dem Boden liegenden 10-Euro-Geldscheins abgelenkt, währenddessen die Diebe schnell Ihr Geld aus dem Automaten stehlen.

  Diese Betrugsformen kommen vor allem in Geschäften oder an Geldautomaten vor. So genannte Topfgucker schauen Ihnen über die Schulter, während Sie die Geheimzahl eintippen und Kriminelle versuchen, Sie auf verschiedene Weise abzulenken.

Betrug anhand Ihres Computers

- **Phishing**
  Im Betrugsfall durch Phishing entlocken Ihnen Kriminelle über eine SMS oder E-Mail oder aber über eine betrügerische Website Ihre Sicherheitscodes. Über eine SMS oder E-Mail erhalten Sie die Aufforderung, einen Link anzuklicken. Ohne Ihr Wissen landen Sie auf einer betrügerischen Website von beispielsweise das ING Commercial Card Portal, wo Sie gebeten werden, sich mit Ihren Sicherheitscodes einzuloggen. Daher - klicken Sie niemals Ihnen suspekte Links an, sondern entfernen Sie diese E-Mail direkt aus Ihrer Mailbox.

  Phishing-Mitteilungen können Sie an nachstehend genannten Punkten erkennen:
  - In der Mitteilung ist meist ein dringender Grund für die Durchführung einer Handlung enthalten.
  - Sie werden gebeten, einen Link anzuklicken. Ohne Ihr Wissen landen Sie auf einer betrügerischen Website, wo Sie gebeten werden, sich mit Ihren Sicherheitscodes einzuloggen.
  - Die Mitteilung ähnelt häufig einer Mitteilung Ihrer Bank.

- **Malware**
  Malware nennt man Schadsoftware, mit deren Hilfe Kriminelle Ihren Computer beispielsweise aus der Ferne betreiben können. So können sie Ihre Einlogdaten ausfindig machen. Auf einem Computer ohne Antivirussoftware und ohne eine gute Firewall kann Malware problemlos installiert werden. Dies geschieht häufig, ohne dass Sie dies merken. Ein bekanntes Beispiel für Schadsoftware ist ein Trojaner.

Malware können Sie an nachstehend genannten Punkten erkennen:
- Manchmal sehen Internetseiten anders aus, als Sie es gewöhnt sind. Es ist beispielsweise ein zusätzliches Eingabefeld für Ihre Telefonnummer vorhanden.
- Ein mit Malware infizierter Computer ist langsamer und stürzt häufiger ab.

Betrug am Telefon

- **Phishing**
  Auch während eines Telefongesprächs entlocken Ihnen Kriminelle mit Hilfe von Phishing Ihre Sicherheitscodes, wie beispielsweise die Geheimzahl Ihrer Corporate Card, Ihre Einlogdaten von das ING Commercial Card Portal oder andere personenbezogene Daten. Phishing kommt ebenfalls bei SMS, E-Mails und betrügerischen Websites vor.

  Kriminelle geben sich am Telefon für eine andere Person aus. Sie geben sich beispielsweise als ING-Mitarbeiter oder Mitarbeiter eines Computer- oder Software-Unternehmens aus. Sie erzählen eine glaubwürdige Geschichte, auf die Sie meist direkt reagieren sollen. Danach werden Sie von ihnen nach Ihren Sicherheitscodes gefragt. Merken Sie sich bitte, dass ING-Mitarbeiter (oder andere Unternehmen) Sie niemals nach Ihren Sicherheitscodes fragen.

  Zweifeln Sie daran, ob Sie wirklich einen ING-Mitarbeiter am Apparat haben? Fragen Sie ihn dann nach seinem Namen und rufen Sie uns zurück, und zwar **unter der Nummer, die Sie im hinteren Teil der Broschüre finden**. Ein ING-Mitarbeiter hat hierfür volles Verständnis. Wir stellen Sie dann gern zu ihm durch.

  Beispiele für betrügerische Telefongespräche:
  - Ein paar Tage nach dem Eintrag Ihrer Kreditkartendaten in eine Phishing-Mail ruft Ihre Bank an und erzählt Ihnen, dass etwas mit Ihrer Corporate Card nicht in Ordnung ist. Wenn Sie den Anweisungen Folge leisten, indem Sie noch weitere Daten liefern, um das Problem zu beseitigen‘, stellen Sie später auf Ihrem Kontoauszug fest, dass eine betrügerische Handlung mit Ihrer Corporate Card durchgeführt wurde.
  - Sie werden von jemandem angerufen, der sich als Mitarbeiter eines Computer- oder Software-Unternehmens ausgibt. Der Mitarbeiter bittet Sie, eine Website anzuklicken und Software herunterzuladen.
  - Häufig wird behauptet, dass dies für die Sicherheit Ihres Computers erforderlich ist. Die Software, die man Sie bat, herunterzuladen, ist Malware. Wenn Sie diese installieren, sind Ihre Daten, die Sie später eingeben, bei einer Internetabbuchung mit Ihrer Corporate Card gefährdet!
  - Eine Person gibt sich als ING-Mitarbeiter aus und sagt, dass sie Ihre Daten überprüfen muss. Beispielsweise Ihren Benutzernamen und das Passwort des Commercial Card Portals.
  - ING-Mitarbeiter würden Sie so etwas niemals fragen. Geben Sie niemals Ihre Codes/ Passwörter heraus.

3. Was tut ING?

Die vorstehenden Ausführungen enthalten eine Reihe Tipps und Empfehlungen für die sichere Durchführung von Zahlungen. Natürlich sorgt ING anhand von verschiedenen sichtbaren und unsichtbaren Technologien auch dafür, die Nutzung Ihrer Corporate Card sicher zu gestalten.

Sicherheit auf der Corporate Card

- Der Chip auf Ihrer Corporate Card und das Vorsatzstück an der Einführung des Passes eines Geldautomaten verhindern Skimming.

- Wenn Sie mit Ihrer Corporate Card bezahlen, müssen Sie derzeit meist Ihre Geheimzahl eingeben und nicht mehr unterschreiben. Das ist sicherer.

- Zusätzlich zur Kreditkartennummer Ihrer Corporate Card weist die Karte auf der Rückseite auch einen so genannten CVC (Card Validation Code - Kartenvalidierungscode) auf. Dieser aus drei Ziffern bestehende Code gilt als zusätzliche Kontrolle.

Sicherheit bei der Durchführung von Zahlungen

- **SMS Security Alert**
  Bei riskanten Abbuchungen, für die eine zusätzliche Verifizierung wünschenswert ist, erhalten Sie ein paar Sekunden nach der Abbuchung per SMS ein Security Alert. In dieser SMS bitten wir Sie um eine Bestätigung der Abbuchung. Sollte etwas nicht korrekt sein, können Sie uns das direkt melden. Dann kann Ihre Kreditkarte zur Verhinderung weiteren Missbrauchs schnell blockiert werden. Die SMS wird von der Nummer +44 78 60 04 74 44 verschickt.
  - Geht es um einen Ihnen bekannten Ankauf, bitten wir Sie, so wie in der SMS genannt zu reagieren. Danach ist kein weiteres Handeln Ihrerseits erforderlich.
  - Geht es um einen Ihnen nicht bekannten Ankauf, bitten wir Sie, so wie in der SMS genannt zu reagieren. ING wird Ihre Corporate Card direkt blockieren und Innen eine zweite SMS mit Zusatzinformationen über die weitere Vorgehensweise schicken.

  Dieser Service ist für jeden Kunden mit einer Corporate Card kostenlos. Das einzige, was wir von Ihnen brauchen, ist Ihre korrekte Handy-Nummer. Rufen Sie unseren Kundendienst an, wenn Sie sicher sein wollen, dass wir diese Nummer bereits von Ihnen erhalten haben.

  Es ist auch gut zu wissen, dass es im Betrugsfall keine Haftungskonsequenzen für Sie gibt, wenn Sie nicht auf die Security SMS reagieren. Ihr Ankauf wird normal abgewickelt. Es hängt von der Situation ab, ob Ihre Karte danach jedoch (vorübergehend) für einen weiteren Ankauf blockiert wird.

- **Mastercard ID check**
  Internetankäufe bei Unternehmen, die Mastercard ID checkTeilnehmer sind, werden im Hintergrund gegen Missbrauch geschützt. Sie sehen dann einen Bildschirm mit dem Text ‚Verarbeiten'. Meist führt ING alle Sicherheitskontrollen im Hintergrund durch, bei manchen Abbuchungen jedoch werden wir Sie bitten, einen einmalige Code einzugeben. Diesen Code erhalten Sie per SMS. Machen Sie es sich selbst und uns leicht, indem Sie dafür sorgen, dass wir Ihre Handy-Nummer haben.

- **Blockieren der Card**
  Unter (sehr) verdächtigen Umständen kann ING entscheiden, Ihre Corporate Card vorsorglich zu blockieren. Sie werden hierüber schnellstmöglich per Telefon, SMS oder brieflich informiert. Sollten Sie feststellen, dass Ihre Abbuchung nicht gelingt, dann nehmen Sie bitte direkt Kontakt zu uns auf.

4. Betrug, was nun?

ING tut alles dafür, zu verhindern, dass Sie zum Betrugsopfer werden. Und wenn Sie die in dieser Broschüre enthaltenen Tipps und Empfehlungen so weit wie möglich beherzigen, dann haben Kriminelle nur eine geringe Chance, eine betrügerische Handlung mit Ihrer Corporate Card durchzuführen. Sollten Sie doch einem Betrug zum Opfer gefallen sein, dann bringen wir diese Situation für Sie gern und schnell in Ordnung. Gehen Sie daher folgendermaßen vor:

Betrug melden

- **Schnellstmöglich**
  Melden Sie uns einen Betrug (die Vermutung eines solchen) so schnell wie möglich telefonisch. Dies ist 24 Stunden pro Tag, sieben Tage die Woche möglich. Tun Sie das auf jeden Fall spätestens 30 Tage nach dem Datum Ihres Kontoauszugs (Digital- oder Papierversion). Mittels einer schnellen Meldung können wir in den meisten Fällen vermeiden, dass der Betrag von Ihnen oder von dem Unternehmen eingezogen wird. So vermeiden Sie unvorhergesehene finanzielle Konsequenzen für Sie oder das Unternehmen. Auch können wir Ihnen dann direkt eine neue Corporate Card zuschicken.

- **Betrugsformular**
  Nach der telefonischen Meldung übersenden wir Ihnen per Post oder auf Wunsch per E-Mail ein Betrugsformular. Unsere Bedingung: Bitte schicken Sie uns das Formular in spätestens 14 Tagen zurück. Je schneller Sie die ausgefüllten Formulare zurückschicken, desto früher kann die Betrugsmeldung abgewickelt werden. Manchmal kann es erforderlich sein, dass wir zusätzliche Informationen von Ihnen benötigen, wenn der Geschäftsinhaber, bei dem der Missbrauch erfolgt ist, diese beantragt.

- **Protokoll**
  Wenn mit Ihrer Corporate Card ein Betrug begangen wurde, wenn diese als verloren, gestohlen, nicht erhalten oder nicht von Ihnen beantragt gilt, müssen Sie zu dem Betrugsformular ein von der Polizei erstelltes Protokoll hinzufügen.

Schadenersatz

- **Unsere Vorgehensweise**
  Wenn Ihnen nichts vorgeworfen werden kann, wird für Betrug immer Schadenersatz geleistet. Bei dem Telefongespräch wird unser Mitarbeiter so weit wie möglich dafür sorgen, dass Ihnen keine Kosten entstehen. In manchen Fällen, (beispielsweise wenn der Einzugsauftrag bereits von uns weitergeleitet wurde), können wir dies jedoch nicht mehr vermeiden. Wir werden immer mit Ihnen Rücksprache zu der Situation halten, so dass die Erstattung schnellstmöglich geregelt wird.

  Auf der Grundlage Ihrer schriftlichen Erklärung und der von uns durchgeführten Untersuchung bezüglich des Missbrauchs Ihrer Corporate Card wird die Erstattung definitiv festgelegt. Wir werden Sie diesbezüglich immer schriftlich informieren.

5. Glossar

A

Anti-Spyware
Anti-Spyware ist eines der Hilfsmittel zum Schutz Ihres Computers. Diese Software sorgt dafür, dass keine unerwünschten Programme installiert werden, die Ihre personenbezogenen Daten verbreiten können.

Antivirussoftware
Siehe unter „Virusscanner“.

Aufdeckung
Aufdeckung ist das Aufspüren von verdächtigen Handlungen. ING verfügt über ein Expertenteam, das sich tagein tagaus mit der Sicherheit beim Bezahlen beschäftigt. Wir analysieren ständig verdächtige Abbuchungen und Vorgänge. Und wir treten, wenn erforderlich, in Aktion. ING arbeitet eng mit Polizei, Behörden und anderen Organen - auf nationaler und internationaler Ebene - zusammen. Auf diese Weise können wir Sie so schnell und so gut wie möglich informieren.

B

Betriebssystem
Computer, Tablets oder Smartphones können nur dann korrekt funktionieren, wenn sie über Software verfügen. Software, die für das korrekte Funktionieren der Geräte geschrieben wurde, wird ein Betriebssystem genannt.

Betrug
Sie können in verschiedener Hinsicht Opfer eines Betrugs werden. Diese Broschüre ist zu dem Zweck erarbeitet worden, Sie über Betrug zu informieren.

Botnet
Ein Botnet ist ein aus sehr vielen Computern bestehendes Netz, das durch einen Trojaner oder ein Virus infiziert wurde. Hierdurch wird der Computer zu einer Art Roboter, der selbständig und automatisch arbeiten kann. Die infizierten Computer können sich überfall befinden. Auch Ihr Computer kann dazugehören. Kriminelle können daraufhin all diesen Computern auf einmal einen Auftrag erteilen. Die Computer werden dann beispielsweise für die Versendung von Phishing-E-Mails benutzt. Oder um Ihre Corporate Card-Daten abzufangen.

Browser
Ein Browser ist ein Computerprogramm, mit dem Sie sich im Internet Websites anschauen können. Bekannte Browser sind Internet Explorer, Chrome, Firefox und Safari.

C

Commercial Card App
Die Commercial Card App is die offizielle App für Ihre Corporate Card. Damit können Sie direkt Ihre Abbuchungen (höchstens der letzten 12 Monate) anschauen. Suchen Sie zum Herunterladen im Apple App Store sowie in Google Play (Android) unter dem Begriff ‚ING Commercial Card App‘.

Commercial Card Portal
Anhand von das ING Commercial Card Portal können Sie Ihre Corporate Card-Kontoauszüge der letzten 12 Monate digital wiederfinden. Sie können sich die Kontoauszüge herunterladen und

sie an einem von Ihnen gewünschten digitalen Ort speichern. Hierdurch brauchen Sie keine Papierkopien zu archivieren.

Computervirus
Siehe unter „Virus“.

Cookie
Ein Cookie ist eine kleine Datei, die von einer Website auf Ihren Computer gesetzt wird. Mit dieser wird Ihr Surfverhalten gespeichert. Viele Online-Shops benutzen Cookies, so dass Ihre Daten bei einem weiteren Besuch bereits eingetragen sind.

CVC
CVC steht für Card Validation Code (Kartenvalidierungscode). Es handelt sich hierbei um einen aus drei Ziffern bestehenden Sicherheitscode, der auf der Rückseite Ihrer Corporate Card rechts neben dem Unterschriftsfeld steht. Nach diesem Code kann gefragt werden, wenn Sie mit Ihrer Corporate Card eine Internetzahlung durchführen.

Cybercrime
Unter Cybercrime versteht man Internet-Kriminalität. Dabei verschicken Kriminelle E-Mails, in denen sie Sie nach Ihren Einlogdaten und/oder Kreditkartendaten fragen (Phishing) und Websites erstellen, die stark den ING-Websites ähneln. Auch versuchen sie, Ihre personenbezogen Daten von Ihrem Computer zu stehlen. Dies tun sie anhand eines Virus, das sie mit einem anderen Programm (einem so genannten Trojaner) mitschicken.

D

DDoS-Attacke
Bei einer DDoS-Attacke wird eine Internetsite mit Datenverkehr bombardiert. Dieser unerwünschte Datenverkehr wird von der Firewall abgewehrt. Zu dem Zeitpunkt, an dem der unerwünschte Datenverkehr extrem hoch wird, ist die Firewall so sehr mit der Abwehr dieses unerwünschten Verkehrs beschäftigt, dass auch die erwünschten Besucher die Website nicht mehr erreichen können. ING setzt Sicherheitsmaßnahmen auf einem sehr hohen Niveau ein. Diese Maßnahmen richten sich darauf, den unerwünschten Datenverkehr vom erwünschten Datenverkehr zu trennen.

E

EMV-Chip
Der EMV-Chip ist seit ein paar Jahren der auf Ihrer Corporate Card befindliche Chip. Hierdurch können Sie jetzt beispielsweise in Geschäften mit Ihrer Corporate Card und Ihrem Pincode bezahlen. Der EMV-Chip ist ein internationaler Standard, der weltweit eingesetzt wird. Der Chip senkt den Betrug mit Kreditkarten in Geschäften. Sie brauchen somit Ihre Corporate Card nicht mehr durch den Magnetstreifenkartenleser zu ziehen, sondern stecken die Corporate Card in das POS-Terminal. So wird der EMV-Chip gelesen.

Erweiterung
Eine Erweiterung ist eine zusätzliche Anwendung für Ihren Browser, die Sie selbst herunterladen können. Hiermit ist es möglich, neue Funktionen zu Ihrem Browser hinzuzufügen. Beispiele für Erweiterungen sind Adobe Reader für das Lesen von PDF-Dateien und Flash für das Anschauen von YouTube-Videos.

F

Firewall
Eine Firewall ist eines der Hilfsmittel zum Schutz Ihres Computers. Diese Software trägt dazu bei, zu verhindern, dass andere Personen Zugang zu Ihrem Computer erhalten, wenn dieser

an das Internet oder ein Computernetz angeschlossen ist. Eine Firewall kontrolliert den ein- und ausgehenden Internetverkehr. Sie erhalten bei einem zweifelhaften Datenaustausch eine Benachrichtigung.

G

Geldkurier
Ein Geldkurier stellt sein Bankkonto für kriminelle Tätigkeiten zur Verfügung. Kriminelle zahlen Geld auf das Bankkonto ein, leiten es an andere Konten weiter oder heben es in bar ab. Auf diese Weise können sie das gestohlene Geld vor der Polizei und Justiz verbergen.

Gefälschte E-Mail
Siehe unter ‚Phishing'.

I

Identitätsbetrug
Identitätsbetrug bedeutet, dass Kriminelle Ihre persönlichen und finanziellen Daten sammeln und diese später missbräuchlich benutzen. Stereotype Gewohnheiten, wie das arglose Wegwerfen von finanziellen Informationen, von Kontoauszügen Ihrer Corporate Card, von einer Unterschrift oder einer Kopie Ihres Personalausweises können zu einem Identitätsbetrug einladen. Aber auch mit Hilfe von Phishing und Social Engineering bekommen Kriminelle personenbezogene Daten in die Hand. Danach kann ein Krimineller beispielsweise in Ihrem Namen eine Kreditkarte beantragen.

Internetkriminelle
Internetkriminelle beschäftigen sich mit Kriminalität im Internet. Somit verschicken sie E-Mails, in denen sie nach Ihren Einlogdaten und/oder Kreditkartendaten fragen (Phishing). Auch erstellen Internetkriminelle Websites, die der ING-Website stark ähneln. Oder aber sie versuchen, Ihre personenbezogen Daten von Ihrem Computer zu stehlen. Dies tun sie anhand eines Virus, das sie mit einem anderen Programm (einem so genannten Trojaner) mitschicken.

J

Jailbreaken
Unter Jailbreaken versteht man die Umgehung einer Sicherheitsmaßnahme des Betriebssystems von einem Iphone, Ipod touch oder iPad. Indem ein Jailbreak an dem Gerät vorgenommen wird, kann der Nutzer beispielsweise Apps installieren, die nicht von Apple genehmigt wurden. Hierdurch ist ein solches Gerät anfälliger für Viren und Malware.

M

Malware
Malware ist ein Sammelbegriff für Schadsoftware. Das Wort ist eine Zusammenfügung des englischen Begriffs ‚malicious software' (böswillige Software). Malware wurde speziell zu dem Zweck entwickelt, in einen Computer einzudringen, ohne dass Sie das selbst bemerkt haben müssen. Malware kann beispielsweise über E-Mail oder Abbildungen auf Websites in Ihren Computer eindringen.

MasterCard ID check
Siehe das Kapitel ‚Was tut ING?'

N

NCSC
Nationaal Cyber Security Centrum. Kooperation von Behörden und Unternehmen. Mission: Das NCSC trägt zu einer gemeinsamen Erhöhung der Widerstandsfähigkeit der niederländischen Gesellschaft in der digitalen Domäne bei, und damit zu einer sicheren, offenen und stabilen Informationsgesellschaft, indem das Verständnis gefördert und Handlungsperspektiven geboten werden.

P

Passwort
Zur sicheren Abwicklung von Bankgeschäften gehört ein starkes Passwort. Ein Passwort ist stark, wenn es nicht geraten werden kann und schwer zu knacken ist. Verwenden Sie daher für all Ihre Online-Bereiche starke Passwörter.

Phishing
Unter Phishing versteht man das ‚Angeln' nach Ihren personenbezogenen Daten von Kriminellen. Diese haben nur ein Ziel: Informationen über Ihre Corporate Card zu erhalten und damit Abbuchungen vorzunehmen. Das ist per E-Mail, Telefon oder Website möglich. Sie werden beispielsweise gebeten, einen Link in einer betrügerischen Website anzuklicken. Die Mitteilung ähnelt verblüffend den Mitteilungen von ING. Ohne Ihr Wissen landen Sie auf einer betrügerischen Website, auf der Sie Daten Ihrer Corporate Card weiterleiten. Ohne dass Sie etwas davon ahnen, können Kriminelle jetzt mit Ihrer Corporate Card Abbuchungen vornehmen.

R

Ransomware
Unter Ransomware versteht man eine Erpressermethode mit Hilfe von Malware. Ransomware ist ein Programm, das Ihren Computer blockiert und danach Geld fordert, um den Computer wieder zu ‚befreien'. Zahlungen (beispielsweise mit Ihrer Corporate Card) sorgen jedoch nicht für eine ‚Befreiung' Ihres Computers, da die Kriminellen nur auf Ihr Geld aus sind.

Rooten
Unter Rooten versteht man die Umgehung einer Schutzmaßnahme des Betriebssystems eines Android-Telefons oder Android-Tablets. Indem das Gerät gerootet wird, kann der Nutzer beispielsweise Apps installieren, die nicht für den Android Markt genehmigt wurden. Hierdurch ist ein solches Gerät anfälliger für Viren und Malware.

S

Security Alert Service
Siehe das Kapitel ‚Was tut ING?'

Sicherheitsexperte
Wir verfügen über ein Expertenteam, das ständig suspekte Abbuchungen und Tätigkeiten analysiert. Wir treten, wenn erforderlich, in Aktion. ING arbeitet eng mit Polizei, Behörden und anderen Organen, wie der niederländischen Bankenvereinigung (Nederlandse Vereniging van Banken) zusammen.

Skimming
Unter Skimming versteht man das Kopieren der Daten Ihrer Corporate Card, indem ein zusätzliches Kartenlesegerät auf der Einführung des Passes an einem Geldautomaten oder einem POS-Terminals installiert wird. Kriminelle schauen sich danach Ihre persönliche Geheimzahl ab, wonach sie mit den geskimmten Daten Geld abheben. Durch das Anbringen spezieller Vorsatzstücke an der Einführung des Passes an Geldautomaten versucht ING zu vermeiden, dass Kriminelle Kartenlesegeräte installieren können. Zudem werden Geschäftsinhaber ermutigt, regelmäßig zu kontrollieren, ob Kriminelle vielleicht ihr POS-Terminal manipuliert haben.

Smishing
Unter Smishing versteht man Phishing mit Hilfe von SMS. Siehe unter ‚Phishing'.

Social Engineering
Beim Social Engineering versuchen Kriminelle, Ihnen vertrauliche Informationen zu entlocken. Sie missbrauchen menschliche Eigenschaften wie Neugier, Vertrauen, Profitgier, Angst und Unwissenheit. Social Engineering kennt viele Formen. Von falschen Websites bis hin zu Phishing E-Mails und von Telefongesprächen bis hin zum persönlichen Kontakt an der Haustür. Kriminelle lassen Sie eine bestimmte Handlung ausführen, wie das Eintragen personenbezogener Daten, Sicherheitscodes oder Kreditkartendaten, das Drücken einer Taste oder die Installierung von Malware.

Spyware
Unter Spyware versteht man Software, die (unbemerkt) auf einem Computer installiert wird. Hiermit können Daten über den Nutzer gesammelt und an Dritte weitergeleitet werden.

Strohmann
Siehe unter ‚Geldkurier'.

T

Trojaner (oder trojanisches Pferd)
Trojaner leitet sich ab von Trojan Horse (trojanischem Pferd). Ein Trojaner ist ein Programm, das auf Ihrem Computer als unschuldige Datei ‚maskiert' installiert wird. Hiermit haben Kriminelle aus der Ferne Zugang zu Ihrem Computer. Dies geschieht, ohne dass Sie selbst dies merken. Mit Hilfe von Trojanern können sie beispielsweise Ihren Benutzernamen und das Passwort des ING Commercial Card Portals ausfindig machen.

V

Virus
Ein Virus ist eine Form von schädlicher Software. Viren können in Ihrem Computer ernste Schäden verursachen, wodurch (vertrauliche) Informationen gelöscht werden. Auch können Kriminelle mit Hilfe eines Virus auf einem Computer mitlesen und so Ihren Benutzernamen und Ihr Passwort ausfindig machen.

Virusscanner
Ein Virusscanner ist eines der Hilfsmittel zum Schutz Ihres Computers. Diese Software kontrolliert, ob Ihr Computer Viren enthält und kann diese Viren entfernen.

Vorsatzstück
Ein Vorsatzstück wird an der Einführung des Passes eines Geldautomaten angebracht. Hierdurch können Kriminelle kein Kartenlesegerät installieren, das die Daten der Kreditkarten kopiert. Das Kopieren von Kreditkartendaten nennt man Skimming. Das Vorsatzstück kann für jeden Geldautomatentyp anders aussehen. Auf dem Bildschirm des Geldautomaten ist das geeignete Vorsatzstück zu sehen.

Vorsorgliches Blockieren
Zwecks der Wahrung der Sicherheit im Zahlungsverkehr ergreift ING in suspekten Situationen direkt Maßnahmen. Zum Schutz Ihrer Corporate Card können wir diese vorsorglich blockieren. Dies tun wir beispielsweise, wenn wir vermuten, dass Ihre Corporate Card dem Skimming zum Opfer gefallen ist. Dann blockieren wir Ihre Kreditkarte und versuchen, direkt Kontakt mit Ihnen aufzunehmen.

W

WiFi
WiFi ist die englische Abkürzung für ein drahtloses Netz. Über das drahtlose Netz können Sie ins Internet gelangen.

Wurm
Ein Wurm versucht, sich selbst über die Netze zu verbreiten. Ein Wurm wandert automatisch, wie bei einer Kettenreaktion. Meist geschieht dies über E-Mail-Adressen, die auf einem infizierten Computer angetroffen werden.

Z

Zehnertrick
Kriminelle versuchen, jemanden abzulenken, der im Begriff ist, Geld aus einem Automaten abzuheben, indem sie einen Zehner zu Boden fallen lassen. Diese Kriminellen sagen dann, dass Sie den Geldschein haben fallen lassen, stehlen jedoch inzwischen Ihr Geld aus dem Automaten.

Zugangscode
Auf Ihrem Computer oder Telefon/Tablet können Sie selbst einen Code einstellen, so dass andere diese Geräte nicht einfach benutzen können.

6. Wichtige Telefonnummern

Im Betrugsfall oder wenn Sie einen Betrug vermuten, können Sie uns 24 Stunden pro Tag, sieben Tage die Woche erreichen, und zwar unter

+31 (0)10 428 95 81

oder über unsere Nummern zum Lokaltarif. Diese Nummern finden Sie unter:

www.ingwb.com/cardcontact

Zögern Sie nicht, wir stehen für Sie bereit!

ING Bank N.V. hat ihren satzungsmäßigen Sitz in 1102 MG Amsterdam, Bijlmerplein 888, und ist eingetragen im niederländischen Handelsregister unter der Nummer 33031431. ING Bank N.V. ist bei De Nederlandsche Bank (DNB) und der niederländischen Finanzaufsichtsbehörde (AFM) im niederländischen Register der Kredit- und Finanzinstitute eingetragen. Außerdem unterliegt die ING Bank N.V. den Regulierungsbestimmungen der niederländischen Verbraucherschutzbehörde [Autoriteit Consument & Markt (ACM)]. Auskünfte bezüglich der Aufsicht über die ING Bank N.V. sind bei der DNB (www.dnb.nl), der AFM (www.afm.nl) oder der ACM (www.acm.nl) erhältlich.

ING