Utilisez votre ING Corporate Card en toute sécurité

Introduction

Avec votre ING Corporate Card, vous pouvez payer, entre autres, vos chambres d'hôtel, congrès, billets d'avions, restaurants et taxis. Mais la Corporate Card vous offre encore bien d'autres possibilités.

Pensez par exemple aux agences de voyage qui, pour leurs réservations, ont opté pour la facilité de la Corporate Card. Les utilisateurs de la Card sont de plus en plus nombreux en raison de la facilité et de la sécurité offertes par cette manière de payer (professionnellement).

Naturellement, vous voulez être certain(e) que vos pays interviennent sans problème. Vous trouverez dans ce document des informations supplémentaires sur cette question. ING fait tout pour rendre les paiements sûrs et pour maintenir leur sécurité. Mais nous ne pouvons pas faire cela seuls. Si vous respectez les règles de base, vous réduisez les chances des délinquants.

Dans cette brochure, nous vous expliquons ces règles de base, nous vous donnons des astuces vous permettant de payer en toute sécurité et de reconnaître les fraudes, et nous vous expliquons ce que fait ING pour que vous puissiez utiliser votre Corporate Card de la manière la plus sure possible. Vous trouverez au dos une liste de notions avec une explications des termes (internet) utilisés dans cette brochure.

Pratique et gratuit

Utilisez l'application ING Commercial Card et utilisez le portail ING Commercial Card. Vous conservez ainsi une vision de vos transactions, de vos relevés de compte, de vos dépenses totales, de votre solde et de votre limite restante. Vous trouverez l'application ING Commercial Card dans l'Apple App Store et sur Google Play (Android).
Pour trouver l'application, tapez : ING Commercial Card app
Vous trouverez le portail ING Commercial Card sur : www.ingcommercialcard.com

Signalez les fraudes immédiatement

Vous avez été victime d'une fraude avec votre Corporate Card ? Signalez-le nous immédiatement. Ainsi, nous pourrons aider d'autres clients, maintenant et à l'avenir. Vous pouvez nous joindre 24 heures par jour et 7 jours par semaine, y compris depuis l'étranger et en utilisant nos numéros d'accès locaux. Vous les trouverez au dos.

Sommaire

1. Les cinq règles de base pour payer en toute sécurité

Nous avons transposé pour vous les règles de sécurité uniformes des banques néerlandaises en cinq règles de base pour l'utilisation de votre Corporate Card. Vous pourrez ainsi les retenir facilement.

Règle de base 1 : Protégez vos codes

Vous ne donnez pas les clefs de chez vous au premier venu. Agissez de même avec vos codes de sécurité. Protégez les correctement.

- **Retenez vos codes**
  Choisissez des codes de sécurité/mots de passe qui ne soient pas une année de naissance, un nom d'un membre de la famille, ou un autre code qui soit facile à deviner. Vous avez peur d'oublier vos codes ? Notez les d'une manière qui ne permette pas à d'autres personnes de les déchiffrer et essayez d'imaginer un moyen mnémotechnique. Il est ainsi facile de retenir une phrase avec des majuscules et des chiffres. Par exemple : « Plutôt U2 que la 6e de Beethoven ! » S'il n'est pas possible d'utiliser toute la phrase, prenez la première lettre de chaque mot : 'LU2dd6evB!'

- Il est également possible, pour retenir le code nip de votre Corporate Card et choisir un mot pour chaque chiffre du code nip, le nombre de lettres correspondant au chiffre. Vous faites ensuite une phrase avec les 4 mots. Imaginez que votre code nip soit : 9246. Vous pouvez ainsi par exemple composer la phrase : Cassandre (9) me (2) veut (4) revoir (6).

- **Ne laissez personne vous observer**
  Veillez à ce que personne ne vous observe lorsque vous introduisez votre code. Vous pouvez le faire, par exemple, en protégeant le clavier de votre corps ou de votre main libre.

- **Ne donnez jamais vos codes**
  Quelqu'un vous demande vos codes de sécurité ou vos mots de passe, par exemple pour le portail ING Commercial Card ? Ne le communiquez jamais. Vos codes sont strictement personnels. Par conséquent, ne les révélez à personne et retenez que jamais des collaborateurs d'ING de vous demanderont vos codes de sécurité : ni au guichet, ni au téléphone, ni par e-mail, ni par l'intermédiaire d'un autre site internet ou d'une autre application que ceux d'ING, ni d'aucune autre manière.

Règle de base 2 : Surveillez votre Corporate Card

Vous ne laissez pas traîner votre porte-monnaie. Ne laissez pas non plus traîner votre Corporate Card. Surveillez-la bien.

- **Agissez avec prudence avec votre Corporate Card**
  Votre Corporate Card est strictement personnelle. Par conséquent, ne la prêtez pas. Ne laissez votre Corporate Card traîner nulle par, et rangez immédiatement après utilisation dans un lieu fixe et sûr. Veillez à ce que votre Corporate Card ne puisse pas vous être soustraite sans que vous vous en rendiez compte.

  Par exemple, plutôt que de remettre votre Corporate Card à un serveur, accompagnez celui-ci jusqu'au terminal de paiement. Peut-être avez-vous quand même besoin, de temps à autre, de remettre votre Corporate Card à quelqu'un. Dans ce cas, vérifiez que c'est bien la même carte qui vous est rendue.

Vérifiez au moins une fois par jour que vous êtres bien en possession de votre Corporate Card. Cette une obligation qui figure également dans nos conditions.

- **Ne vous laissez pas distraire**
  Ne vous laissez pas distraire lorsque vous utilisez votre Corporate Card. Si vous ne faites pas attention, il est par exemple possible de remplacer votre Corporate Card par une carte de crédit de la même couleur. C'est ce que nous appelons le subterfuge de la substitution. Si vous avez l'impression qu'il n'est pas possible d'utiliser votre carte bancaire, suivez votre impression et laissez votre Corporate Card là où elle est, en sécurité.

- **Contrôlez régulièrement si vous avez encore votre Corporate Card**
  Une personne que vous ne connaissez pas s'adresse à vous dans la rue ? Quelqu'un vous heurte ? Contrôlez alors toujours si vous avez encore votre Corporate Card. Vous ne la retrouvez pas après avoir payé ? Dans ce cas contactez-nous immédiatement (24 heures par jour, 7 jours par semaine) au +31 (0)10 428 95 81 à l'un de nos numéros d'accès locaux (vous les trouverez au dos).

Règle de base 3 : Sécurisez vos appareils

Vous fermez votre porte d'entrée à clef. Faites de même avec les appareils que vous utilisez pour vos transactions internet avec votre Corporate Card, comme votre téléphone, votre tablette, votre ordinateur fixe ou votre ordinateur portable. Protégez-les donc bien. Cela réduira ainsi les possibilités pour les malfaiteurs d'installer des logiciels malveillants et de récupérer vos données personnelles, comme les données de votre Corporate Card, au moyen d'un « Cheval de Troie ».

- **N'installez que des logiciels légaux et connus**
  Veillez à configurer votre téléphone soit paramétré de telle sorte que les applications provenant de sources inconnues ne soient pas autorisées. Par conséquent, ne « rootez » pas et ne « jailbreakez » pas votre téléphone, et n'utilisez que des applications provenant d'app-stores officiels. N'installez que des logiciels légaux dont vous avez contrôlé la source. Vous pouvez le faire en visitant le site web officiel du fournisseur. On vous propose un logiciel inconnu ? Ne téléchargez pas immédiatement le programme, mais contrôlez-le d'abord à l'aide de votre scanneur anti-virus.

- **Utilisez la version la plus récente de votre app et de votre système d'exploitation**
  L'application ING Commercial Card et le système d'exploitation de votre téléphone, de votre tablette et de votre ordinateur sont régulièrement modifiés grâce à des techniques de sécurité plus nombreuses et de meilleure qualité. Par conséquent, faites des mises à jour régulières. Paramétrez de préférence des mises à jour automatiques.

- **Paramétrez un code d'accès sur vos appareils**
  Avec un code d'accès, vous empêcher les tiers d'avoir facilement accès à vos données personnelles. Pensez non seulement à vos données Corporate Cards, mais aussi à vos contacts, messages et photos.

- **Utilisez un scanneur anti-virus, un pare-feu et un anti-spyware**
  N'utilisez qu'un ordinateur fixe ou un ordinateur portable équipé d'un scanneur anti-virus, d'un pare-feu et d'un anti-spyware pour effectuer des paiements par internet avec votre Corporate Card. Cela limite les possibilités d'action des virus et programmes indésirables. Il existe en outre maintenant des scanneurs de virus pour téléphones et tablettes, qui offrent une protection supplémentaire.

- **Sécurisez votre liaison internet sans fil (wifi)**
  Sans liaison internet sécurisée, vous ne pouvez faire aucune transaction internet sure avec votre Corporate Card. Pour cette raison, protégez votre propre wifi par un mot de passe. Pour cela, votre fournisseur de services internet peut vous aider. Lorsque vous êtes à l'extérieur, peut-être utilisez-vous un réseau wifi public. Dans ce cas, il est préférable que vous n'effectuiez pas de transaction internet avec votre Corporate Card.

Règle de base 4 : Contrôlez vos paiements et débits

Il est toujours important de vérifier attentivement ce que l'on va payer. Et vérifiez aussi régulièrement ce qui est débité. Cela peut se faire par l'intermédiaire de portail ING Commercial Card ou de l'application ING Commercial Card. L'application ING Commercial Card fait notamment apparaître vos transactions en temps réel.

- **Sachez ce que vous payez**
  Contrôlez si le montant que vous devez payer est correctement indiqué sur l'écran ou - si vous êtes à l'étranger et devez encore apposer votre signature sur le ticket - si le montant exact est indiqué. Conserver la copie du ticket pour votre propre comptabilité. Vous avez ainsi toujours une preuve si le montant figurant ensuite sur votre relevé Corporate Card n'est pas exact.

  Faites attention à ne pas être surpris(e) par le montant qui sera débité de votre Corporate Card et qui résulte de la conversion a porsteriori d'un montant initialement exprimé dans une devise étrangère.

- **Faites les choses dans l'ordre**
  Lors d'un achat sur internet, ne renseignez vos données, comme le numéro de carte de crédit, la date d'échéance et les codes de sécurité, que si vous êtes sûr(e) de votre achat.

- **Surveillez en ligne vos débits**
  Contrôlez vos débits au moins une fois toutes les deux semaines. Vous pouvez ainsi juger si les transactions sont légitimes ou non et nous informer immédiatement en cas d'abus.

- **Signalez les dommages en temps opportun**
  Si un dommage survient du fait qu'il vous a été impossible pendant un certain temps de contrôler vos relevés de compte Corporate Card, nous pouvons vous demander de le démontrer. Le dommage qui est signalé dans un délai de plus de trente jours après la date de votre relevé n'est en principe pas indemnisé.

Règle de base 5 : En cas de doute, téléphonez à ING

Si vous êtes sûr(e) ou vous pensez avoir été victime d'une fraude, dites-le nous immédiatement. Si vous nous contactez, nous pouvons directement intervenir et prévenir un dommage éventuel. Nous faisons par exemple fermer de faux sites web, afin que d'autres clients ne soient pas victimes de fraude.

- **Téléphoner immédiatement**
  Si vous soupçonnez une fraude, vous pouvez nous téléphoner immédiatement. Y compris si votre Corporate Card, votre application ING Commercial Card ou votre user-ID de portail ING Commercial Card ont été bloqués. Ou si vous avez reçu un e-mail suspect ou si quelqu'un a essayé de vous soutirer des données relatives à votre Corporate Card.

- **Veillez à ce que nous puissions vous joindre**
  En cas de transactions suspectes, nous voulons pouvoir vous joindre rapidement, par téléphone ou par sms. C'est pourquoi nous vous invitons à communiquer votre numéro de téléphone portable à notre service clients. Pour ce faire vous pouvez téléphoner au +31 (0)10 428 9581 ou à nos numéros d'accès locaux (vous les trouverez au dos).

2. Reconnaître les fraudes

Malgré les mesures de sécurité que vous appliquez et votre utilisation prudente de votre Corporate Card, il reste toujours un risque que celle-ci subisse une fraude. Les informations ci-dessus vous aideront à identifier les différentes formes de tentatives de fraude.

Fraude par l'intermédiaire de votre Corporate Card

- **Skimming**
  Une forme de fraude connue est le skimming, qui consiste à copier les données de la carte de crédit qui figurent sur la bande magnétique. Au cours des dernières années, différentes mesures contre le skimming ont été adoptées. C'est la raison pour laquelle cette forme de fraude se fait plus rare.

- **Vol, subterfuges de substitution et manœuvres de diversion**
  Il arrive encore que des Corporate Cards soient échangées contre d'autres cartes ou volées, et que les codes de sécurité soient observés lorsqu'ils sont composés. Il arrive également que des personnes soient distraites au distributeur de billets et que des malfaiteurs s'en aillent avec l'argent remis par le distributeur. Le truc du billet de dix euros en est un exemple. Vous êtes distrait par un billet de 10 euros qui se trouve sur le sol, et les malfaiteurs dérobent rapidement votre argent dans le distributeur.

  Ces formes de fraude se produisent principalement dans les magasins ou à côté des distributeurs de billets. Un observateur regarde par dessus votre épaule pendant que vous composez votre code nip et des malfaiteurs essaient de vous distraire de multiples manières.

Fraude par l'intermédiaire de votre ordinateur

- **Filoutage (Phishing)**
  Dans les fraudes au phishing, les malfaiteurs essaient d'obtenir vos codes de sécurité par l'intermédiaire d'un sms, d'un e-mail ou d'un faux site web. Un sms ou un e-mail vous demande de cliquer sur un lien. Sans vous en apercevoir, vous arrivez sur un faux site web, par exemple de portail ING Commercial Card, où il vous est demandé de vous connecter avec vos codes de sécurité. Par conséquent, ne cliquez jamais sur des liens suspects et supprimer immédiatement l'e-mail de votre messagerie.

  Vous pouvez reconnaître les messages de filoutage aux caractéristiques suivantes :
  - Le message mentionne le plus souvent un motif en vue d'une action urgente.
  - Il vous est demandé de cliquer sur un lien. Sans vous en apercevoir, vous arrivez sur un faux site web où il vous est demandé de vous connecter avec vos codes de sécurité.
  - Le message ressemble souvent au message de votre banque.

- **Logiciels malveillants**
  Les logiciels malveillants sont des logiciels avec lesquels des malfaiteurs essaient par exemple de prendre le contrôle de votre ordinateur. Ils peuvent ainsi retrouver les données de connexion. Il est facile d'installer des logiciels malveillants sur un ordinateur sans logiciel antivirus et sans pare-feu de bonne qualité. Cela arrive souvent sans que vous vous en aperceviez. Un exemple connu de logiciel malveillant est le cheval de Troie.

Vous pouvez reconnaître les logiciels malveillants aux caractéristiques suivantes :
- Les pages internet ont parfois une apparence différente de celle à laquelle vous êtes habitué(e). Il y a par exemple un champ supplémentaire pour votre numéro de téléphone.
- Un ordinateur infecté par un logiciel malveillant est plus lent et se bloque plus souvent.

Fraude par l'intermédiaire du téléphone

- **Filoutage (Phishing)**
  Des malfaiteurs s'adonnent également au filoutage par téléphone en essayant d'obtenir, au moyen d'une conversation téléphonique, vos codes de sécurité, comme le code nip de votre Corporate Card, les données de connexion de portail ING Commercial Card ou d'autres données personnelles. Le filoutage peut également se pratiquer par sms, e-mail ou au moyen de faux sites web.

  Souvent, les malfaiteurs se présentent au téléphone en se faisant passer pour quelqu'un d'autre. Par exemple pour un collaborateur d'ING ou d'une entreprise d'informatique ou de logiciels. Ils exposent le plus souvent une histoire plausible à laquelle vous devez immédiatement réagir. Ils vous demandent ensuite vos codes de sécurité. Retenez que jamais les collaborateurs d'ING (ou d'autres entreprises) ne vous demanderont vos codes de sécurité.

  Vous avez des doutes sur le fait que votre interlocuteur téléphonique soit un collaborateur d'ING ? Demandez-lui son nom et rappelez-nous au numéro de téléphone figurant au dos de cette brochure. Un collaborateur d'ING le comprendra parfaitement. Nous vous mettrons alors volontiers en communication avec lui ou avec elle.

  Exemples de faux appels téléphoniques :
  - Quelques jours après avoir donné vos données de carte de crédit dans un e-mail de filoutage, votre banque vous rappelle en disant qu'il y a un problème avec votre Corporate Card. Vous suivez les indications en fournissant quelques dernières données supplémentaires pour « résoudre le problème », et vous remarquerez ensuite sur votre relevé qu'une fraude a été commise avec votre Corporate Card.
  - Vous êtes appelé par quelqu'un qui se présente comme un collaborateur d'ING ou d'une entreprise d'informatique ou de logiciels. Le collaborateur vous demande de vous rendre sur un site web pour installer des logiciels.
  - L'interlocuteur prétend souvent que cela est nécessaire pour la sécurité de votre ordinateur. Le logiciel que l'on vous demande d'installer est un logiciel malveillant. Si vous l'installez, les données que vous renseignerez pour une transaction internet avec votre Corporate Card seront alors vulnérables !
  - Une personne se présente comme étant un collaborateur d'ING et prétend qu'elle doit vérifier vos données. Par exemple votre nom d'utilisateur et votre mot de passe pour le portail ING Commercial Card.
  - Les collaborateurs d'ING ne demandent jamais cela. Ne donnez jamais vos codes.

3. Que fait ING ?

Dans les développements qui précèdent, nous vous avons donné de nombreux conseils et astuces pour payer en toute sécurité. Naturellement, ING veille aussi, au moyen de techniques invisibles et visibles, à maintenir la sécurité de l'utilisation de la Corporate Card.

Sécurité de la Corporate Card

- La puce intégrée à votre Corporate Card et un dispositif de protection placé sur la goulotte d'introduction du distributeur de billet préviennent le skimming.

- Si vous payez avec votre Corporate Card, on vous demande la plupart du temps un code nip et non une signature. C'est plus sûr.

- En plus du numéro de carte de crédit, votre Corporate Cart possède également au dos de la carte un CVC (Card Validation Code). Ce code à trois chiffres constitue un contrôle supplémentaire.

Sécurité lors des paiements

- **SMS Alerte de sécurité**
  Pour les transactions sensibles pour lesquelles une vérification supplémentaire est souhaitable, vous recevez, quelques secondes après la transaction, une Alerte de sécurité par SMS. Par ce SMS, nous demandons une confirmation de la transaction. Si celle-ci s'avère incorrecte, vous pouvez nous le signaler immédiatement et votre carte de crédit peut être bloquée immédiatement pour éviter tout autre abus. Ce SMS est envoyé depuis le numéro : +44 78 60 04 74 44.
  - S'il s'agit d'un achat connu, réagissez de la manière indiquée dans le SMS. Ensuite, aucune autre action n'est nécessaire.
  - S'il s'agit d'un achat qui vous est inconnu, réagissez de la manière indiquée dans le SMS. ING bloquera immédiatement votre Corporate Card et vous enverra un deuxième SMS contenant des informations supplémentaires sur la conduite à tenir.

  Ce service est gratuit pour tous les clients disposant d'une Corporate Card. La seule chose dont nous avons besoin, c'est un numéro exact de téléphone portable. Appelez notre service clients pour être sûr que nous en disposons bien.

  Il est intéressant de savoir que le fait de ne pas réagir au SMS de sécurité n'entraîne aucune conséquence en matière de responsabilité en cas de fraude. Votre achat se poursuivra. Selon la situation, votre carte peut ensuite être bloquée (provisoirement) pour un achat ultérieur.

- **Mastercard ID check**
  Les achats internet auprès d'entreprises qui participent à Mastercard ID check sont protégés en arrière-plan contre la fraude. Vous verrez apparaître un écran avec le texte « Traitement ». Dans la plupart des cas, ING effectuera les contrôles de sécurité en arrière-plan, mais pour certaines transactions, nous vous demanderons d'introduire un code unique. Vous recevrez ce code par SMS. Facilitez-vous les choses et veillez à ce que nous connaissions votre numéro de téléphone portable.

- **Blocage de la Card**
  Dans les situations (très) suspectes, ING peut décider de bloquer votre Corporate Card à des fins préventives. Vous en êtes toujours averti(e) aussi rapidement que possible par téléphone, par sms ou par lettre. Si vous constatez que votre transaction n'aboutit pas, contactez-nous immédiatement.

4. En cas de fraude, que faire ?

ING fait tout pour éviter que vous soyez victime de fraude. Et si vous suivez autant que faire se peut les conseils et astuces fournis dans cette brochure, les malfaiteurs ont peu de possibilités de commettre une fraude avec votre Corporate Card. Si vous êtes cependant victime de fraude, c'est volontiers que nous règlerons le problème rapidement. Pour cela, agissez de la manière suivante :

Signaler la fraude

- **Aussi rapidement que possible**
  Signalez-nous la (tentative) de fraude aussi rapidement que possible. Cela peut se faire 24 heures par jour et 7 jours par semaine. Faites-le en tout cas au plus tard 30 jours après la date de votre relevé (version numérique ou papier). Un signalement rapide nous permet le plus souvent d'éviter que le montant soit encaissé sur votre compte ou sur celui de l'entreprise. Cela permet d'éviter des conséquences financières imprévues pour vous ou pour l'entreprise. En outre, nous pouvons vous envoyer immédiatement une nouvelle Corporate Card.

- **Formulaire de fraude**
  Après le signalement téléphonique, nous vous enverrons une formulaire de fraude par courrier ou, si vous le souhaitez, par e-mail. Notre condition : renvoyez le formulaire au plus tard dans les 14 jours. Plus vite vous nous renverrez les formulaires et plus votre signalement de fraude pourra être traité rapidement. Il est parfois nécessaire que vous nous fournissiez des informations supplémentaires si le commerçant chez lequel la fraude a eu lieu le demande.

- **Procès-verbal**
  Si une fraude a été commise avec votre Corporate Card alors que celle-ci avait été perdue, volée, non reçues ou non demandée par vous, vous devez joindre au formulaire de fraude un procès-verbal établi par la police.

Indemnisation

- **Notre politique**
  S'il n'y a rien à vous reprocher, la fraude est toujours indemnisée. Lors de l'entretien téléphonique, notre collaborateur veillera autant que faire se peut à ce que vous ne soyez pas pénalisé par la fraude. Dans certains cas (par exemple si nous avons déjà envoyé l'ordre de recouvrement), nous ne pourrons toutefois pas l'empêcher. Nous discuterons toujours de la situation avec vous, afin que l'indemnisation intervienne le plus rapidement possible.

  Sur la base de votre déclaration écrite et de l'enquête que nous aurons menée sur la fraude concernant votre Corporate Card, l'indemnisation prendra un caractère définitif. Nous vous en informerons toujours par écrit.

5. Liste de notions

A

Anti-spyware
L'anti-spyware est un moyen avec lequel vous sécurisez votre ordinateur. Ce logiciel empêche l'installation de programmes non désirés qui peuvent diffuser vos informations personnelles.

Application ING Commercial Card
L'application ING Commercial Card est l'application officielle pour votre Corporate Card. Vous pouvez ainsi directement consulter vos transactions des 12 derniers mois. Vous pourrez télécharger l'application depuis l'Apple App Store ou depuis Google Play (Android) dans « ING Commercial Card app ».

Attaque DDoS
Pendant une attaque DdoS, un site internet est attaqué par un flux de données. Ce flux de données non voulu est retenu par un pare-feu. Au moment où le flux de données non voulu devient extrêmement important, le pare-feu est tellement sous pression dans son action de rétention du flux non voulu qu'il empêche également les visiteurs acceptés de passer. Les mesures de sécurité appliquées par ING sont de très haut niveau. Ces mesures visent à distinguer le flux de données non voulu du bon flux de données.

B

Blocage préventif
Pour garantir la sécurité des paiements, ING prend des mesures immédiates dans les situations suspectes. Pour protéger votre Corporate Card, nous pouvons procéder à un blocage préventif. Par exemple si nous pensons que votre carte a été copiée (skimming). Nous bloquons alors votre carte de crédit et nous essayons de prendre directement contact avec vous.

Botnet
Un botnet est un réseau comprenant un très grand nombre d'ordinateurs et qui est infecté par un cheval de Troie ou un virus. L'ordinateur devient alors une sorte de robot qui peut effectuer un certain travail de manière autonome et automatique. Les ordinateurs infectés peuvent se trouver n'importe où. Votre ordinateur peut également en faire partie. Les malfaiteurs peuvent ensuite donner un ordre à tous ces ordinateurs en une seule fois. Les ordinateurs sont alors utilisés, par exemple, pour envoyer des e-mails de filoutage. Ou pour intercepter vos données de Corporate Card.

C

Cheval de Troie
Ce logiciel s'inspire de Cheval de Troie. Un cheval de Troie est un programme « déguisé » en fichier inoffensif qui est installé sur un ordinateur. Cela permet aux criminels de pénétrer à distance dans votre ordinateur. Cela arrive sans que vous vous en aperceviez. Avec un cheval de Troie, ils peuvent par exemple découvrir votre nom d'utilisateur et votre mot de passe pour le portail ING Commercial Card.

Code d'accès
Vous pouvez vous-même installer un code sur votre téléphone/tablette/ordinateur avec que les tiers ne puissent pas utiliser ces appareils sans votre autorisation.

Commercial Card portail
Avec le portail ING Commercial Card vous pouvez retrouver vos relevés de Corporate Card des 12 derniers mois sous format numérique. Vous pouvez télécharger les relevés et les enregistrer à un emplacement numérique de votre choix. Dès lors, vous n'avez plus besoin d'archiver de versions papier.

Cookie
Un cookie est un petit f ichier qui est installé sur votre ordinateur par un site web. Cela permet d'enregistrer votre comportement en matière de navigation. De nombreux magasins sur internet utilisent des cookies afin que vos données soient déjà remplies en vue d'une visite ultérieure.

CVC
CVC signifie Card Validation Code. Il s'agit d'un code de sécurité de 3 chiffres qui se trouve au dos de votre Corporate Card, sur le côté droit, à côté de votre signature. On peut vous le demander si vous effectuez un paiement par internet avec votre Corporate Card.

Cybercriminalité
La cybercriminalité est la criminalité par internet. Par exemple, les cybercriminels envoient des e-mails dans lesquels ils demandent vos donne de connexion et/ou les données relatives à vos cartes de crédit (filoutage) et ils créent des sites web qui ressemblent fortement aux sites web d'ING. Ils essaient également de récupérer vos données personnelles sur votre ordinateur par l'intermédiaire d'un virus qu'ils envoient avec un autre programme (un cheval de Troie).

D

Détection
La détection est la recherche des actions suspectes. ING possède une équipe d'experts propres qui se consacre quotidiennement à la sécurité des paiements. Nous analysons en permanence les transactions et actions suspectes. Et nous passons à l'action lorsque cela s'avère nécessaire. ING coopère étroitement avec la police, les autorités publiques et d'autres acteurs, nationaux et internationaux. Cela nous permet de vous informer aussi vite et aussi bien que possible.

Dispositif de protection
Un dispositif de protection est un élément protecteur placé sur la goulotte d'introduction du distributeur automatique. Cela empêche les malfaiteurs d'installer des lecteur de cartes permettant de copier les données des cartes de crédit. L'opération consistant à copier les données des cartes de crédit est nommée skimming. Le dispositif de protection peut varier en fonction du type de distributeur automatique. Sur l'écran du distributeur est affiché le dispositif d'introduction correct.

E

Expert en sécurité
Nous avons notre propre équipe d'experts en sécurité qui analyse de manière continue des transactions et actions suspectes. Nous passons à l'action lorsque cela s'avère nécessaire. ING coopère étroitement avec la police, les autorités publiques et d'autres acteurs, comme l'Association néerlandaise des banques (Nederlandse Vereniging van Banken).

Extension
Une extension est une application supplémentaire pour votre navigateur que vous pouvez télécharger vous-même. Cela permet d'ajouter de nouvelles fonctions à votre navigateur. On peut citer comme exemple d'extensions Adobe Reader pour la lecture des fichiers pdf et Flash pour le visionnement des vidéos de YouTube.

F

Faux e-mail
Voir « Filoutage (Phishing) »

Filoutage (Phishing)
Le filoutage (phishing) est l'action par laquelle les malfaiteurs récupèrent vos données personnelles. Avec un objectif : obtenir des informations sur votre Corporate Card et ainsi réaliser des transactions. Cela peut se faire par e-mail, par téléphone ou sur un site web. Il vous est par exemple demandé de cliquer sur un lien se trouvant dans un e-mail mensonger sur son origine. Le message ressemble de manière trompeuse à un message d'ING. Sans vous en rendre compte, vous arrivez sur un faux site web sur lequel vous fournissez vos données Corporate Card. Sans que vous vous en rendiez compte, les malfaiteurs peuvent maintenant effectuer des transactions avec votre Corporate Card.

Fraude
Vous pouvez être victime de fraude de différentes manières. Cette brochure a été rédigée pour vous informer sur la fraude.

Fraude à l'identité
La fraude à l'identité consiste en ce que des malfaiteurs collectent vos données personnelles et financières et en fassent un usage frauduleux. Des habitudes bien ancrées, comme le fait de jeter innocemment des informations financières, des relevés de votre Corporate Card, une signature ou une copie de pièce d'identité, peuvent faciliter la fraude à l'identité. Mais les malfaiteurs obtiennent également des données personnelles au moyen du filoutage et de l'ingénierie sociale. Ensuite, un malfaiteur peut par exemple faire une demande de carte de carte de crédit à votre nom.

H

Homme de paille
L'homme de paille met son compte bancaire à la disposition d'activités criminelles. Les malfaiteurs versent de l'argent sur le compte bancaire, le transfèrent sur d'autres comptes ou prennent l'argent comptant. De cette manière, ils dissimulent de l'argent volé aux yeux de la police et de la justice.

I

Ingénierie sociale
Les malfaiteurs essaient de vous soutirer des informations confidentielles au moyen de l'ingénierie sociale. Ils abusent de caractéristiques de l'être humain comme la curiosité, la confiance, la convoitise, la peur et l'ignorance. L'ingénierie sociale connaît de nombreuses formes. Des faux sites web au filoutage par e-mail, et des entretiens téléphoniques au contact personnel à domicile. Les malfaiteurs vous font exécuter un certain nombre d'actions, comme le renseignement de données personnelles, de codes de sécurité ou de donnés de cartes de crédit, le fait d'appuyer sur un bouton, ou l'installation d'un logiciel malveillant.

J

Jailbreak
Le Jailbreak est le fait de contourner les mesures de sécurité du système d'exploitation d'un iPhone, d'un iPod touch ou d'un iPad. En « jailbreakant » l'appareil, l'utilisateur peut par exemple installer des applications qui n'ont pas été approuvées pour Apple. Cela rend un tel appareil plus vulnérable, par exemple aux virus et logiciels malveillants.

L

Logiciel antivirus
Voir « scanneur antivirus »

Logiciel espion
Un logiciel espion est un logiciel qui (sans être remarqué) est installé sur un ordinateur. Il permet de collecter des informations sur l'utilisateur et de les envoyer à des tiers.

Logiciels malveillants
On désigne par l'appellation de logiciels malveillants les logiciel hostiles et/ou nuisibles. En anglais, ils sont appelés « malware », une contraction de « malicious software ». Les logiciels malveillants sont conçus spécialement pour infiltrer un ordinateur sans même que vous en soyez informé(e). Les logiciels malveillants peuvent par exemple pénétrer dans votre ordinateur par l'intermédiaire d'e-mails ou de photos provenant de sites web.

M

Malfaiteurs sur internet
Les malfaiteurs sur internet s'adonnent à la délinquance sur internet. Ils envoient par exemple des e-mails dans lesquels ils demandent vos données de connexion et/ou les données de vos cartes de crédit (filoutage). Les malfaiteurs sur internet créent également des sites web qui ressemblent fortement aux sites web d'ING. Ou ils essaient de récupérer vos données personnelles sur votre ordinateur par l'intermédiaire d'un virus qu'ils envoient avec un autre programme (appelé cheval de Troie).

MasterCard ID check
Voir le chapitre « Que fait ING ? »

Money mule
Voir « Homme de paille »

Mot de passe
Les opérations bancaires sécurisées nécessite un mot de passe fort. Un mot de passe est fort s'il n'est pas possible de le deviner et s'il est impossible à pirater. Par conséquent, utilisez des mots de passe forts pour tout votre environnement en ligne.

N

Navigateur
Un navigateur est un programme informatique grâce auquel vous pouvez consulter des sites internet. Internet Explorer, Chrome, Firefox et Safari sont des navigateurs célèbres.

NCSC
Nationaal Cyber Security Centrum. Coopération entre autorités publiques et entreprises. Mission : Le NCSC contribue à l'augmentation commune de la résilience de la société néerlandaise dans le domaine numérique, et ainsi à une société de l'information sure, ouverte et stable, en fournissant des informations et en offrant des perspectives d'action.

P

Pare-feu
Un pare-feu est un moyen qui permet de sécuriser votre ordinateur. Ce logiciel aide à empêcher que d'autres personnes aient accès à votre ordinateur lorsque celui-ci est relié à internet ou à un réseau informatique. Le pare-feu contrôle le flux internet entrant et sortant. Vous recevez un avertissement en cas d'échange de données suspect.

Prête-nom
Voir « Homme de paille »

Puce EMV
La puce EMV est depuis quelques années la puce de votre Corporate Card. Grâce à elle vous pouvez par exemple payer avec votre Corporate Card en utilisant un code nip. La puce EMV est la norme internationale qui est utilisée dans le monde entier. La puce réduit la fraude à la carte de crédit dans les magasins. Vous ne passez donc plus votre Corporate Card dans un lecteur de piste magnétique, mais vous insérez votre Corporate Card dans un terminal de paiement. Cela permet de lire la carte EMV.

R

Ransomware
Le ransomware est une méthode de chantage au moyen d'un logiciel malveillant. Le ransomware est un programme qui bloque votre ordinateur et demande ensuite de l'argent pour le « libérer ». Les paiements (par exemple de votre Corporate Card) n'entraînent aucunement une « libération » de votre ordinateur, parce que les malfaiteurs n'en veulent qu'à votre argent.

Rootage
Le rootage est le fait de contourner les mesures de sécurité du système d'exploitation d'un téléphone Android ou d'une tablette Android. En « rootant » l'appareil, l'utilisateur peut par exemple installer des applications qui n'ont pas été approuvées pour le marché Android. Cela rend un tel appareil plus vulnérable, par exemple aux virus et logiciels malveillants.

S

Scanneur antivirus
Un scanneur antivirus est un moyen qui permet de sécuriser votre ordinateur. Le logiciel vérifie la présence éventuelle de virus sur votre ordinateur et peut supprimer ces virus.

Security Alert Service
Voir le chapitre « Que fait ING ? »

Skimming
Le skimming est le fait de copier les données de votre Corporate Card en installant un lecteur de carte supplémentaire sur la goulotte d'introduction d'un distributeur automatique de billet ou d'un terminal de paiement. Les malfaiteurs recherchent ensuite votre code nip personnel, après quoi ils retirent de l'argent avec les données copiées. En installant des dispositifs de protection sur la goulotte d'introduction des distributeurs automatiques de billets, ING essaient d'empêcher que des malfaiteurs puissent placer des lecteurs de cartes. En outre, les commerçants sont encouragés à vérifier régulièrement que des malfaiteurs n'ont pas manipulé leur terminal de paiement.

Smishing
Le smishing est le filoutage (phishing) par sms. Voir « Filoutage (Phishing) »

Système d'exploitation
Un ordinateur, une tablette ou un smartphone ne peuvent fonctionner que s'ils contiennent des logiciels. Le logiciel qui a été écrit uniquement pour faire fonctionner ces appareils est appelé système d'exploitation.

T

Truc du billet de dix euros
Des malfaiteurs essaient de distraire une personne sur le point de retirer de l'argent à un distributeur automatique en jetant par terre un billet de dix euros. Ils lui disent qu'il a perdu un billet et, pendant qu'il est distrait, il vole l'argent sortant du distributeur automatique.

V

Ver
Les vers essaient de se répandre eux-mêmes sur les réseaux. Les vers se déplacent de manière automatique comme dans une réaction en chaîne. Cela se fait la plupart du temps au moyen des adresses e-mail qui sont trouvées sur un ordinateur inspecté.

Virus
Un virus est une forme de logiciel nuisible. Les virus peuvent causer des dommages graves à votre ordinateur, ce qui entraîne la suppression d'informations (confidentielles). Les malfaiteurs peuvent également prendre connaissance du contenu de votre ordinateur au moyen d'un virus et découvrir ainsi votre nom d'utilisateur et votre mot de passe.

Virus informatique
Voir « Virus »

W

WiFi
WiFi est l'abréviation anglaise de réseau sans fil. Le réseau sans fil vous permet de surfer sur internet.

6. Numéros de téléphone importants

En cas (soupçon) de fraude, vous pouvez nous joindre 24 heures par jour et 7 jours par semaine au

+31 (0)10 428 95 81

ou à nos numéros d'accès locaux. Vous pouvez trouver ces numéros sur :

www.ingwb.com/cardcontact

N'hésitez pas, nous sommes là pour vous !

PCM338 0918 © ING Bank N.V.

ING