Veilig gebruik van uw ING Corporate Card

Inleiding

Met uw ING Corporate Card kunt u onder meer hotelovernachtingen, congressen, vliegtickets, restaurants en taxi's betalen. Maar de Corporate Card biedt nog veel meer.

Denk bijvoorbeeld aan reisbureaus die voor boekingen gekozen hebben voor het gemak van de Corporate Card. Steeds meer mensen gebruiken de Card vanwege de gemakkelijke en veilige manier van (zakelijk) betalen.

U wilt er natuurlijk graag zeker van zijn dat uw betalingen goed verlopen. In dit document vindt u daar informatie over. ING doet er alles aan om betalen veilig te maken en te houden. Maar dat kunnen we niet alleen. Houd u aan de basisregels, dan geeft u criminelen weinig kans.

Deze basisregels lichten wij u in deze brochure toe, wij geven tips hoe u veilig kunt betalen en fraude kunt herkennen en leggen u uit wat wij als ING doen om het gebruik van uw Corporate Card zo veilig mogelijk te houden. Achterin vindt u een begrippenlijst met een verklaring van de (internet)termen die in deze brochure worden gehanteerd.

Handig en gratis

Gebruik de ING Commercial Card app en gebruik de ING Commercial Card-portal. Hiermee houdt u zicht op uw transacties, uw rekeningoverzicht, uw totale uitgaven, uw saldo en uw resterende limiet. De ING Commercial Card app vindt u in de Apple App Store en in Google Play (Android). Om de app te vinden, typt u in: ING Commercial Card app
De ING Commercial Card-portal vindt u op: www.ingcommercialcard.com

Meld fraude direct

Bent u het slachtoffer geworden van fraude met uw Corporate Card? Meld dit dan direct bij ons. Dan kunnen wij u en andere klanten helpen, nu en in de toekomst. Wij zijn 24 uur per dag, 7 dagen per week bereikbaar voor u, ook vanuit het buitenland en ook via onze lokale toegangsnummers. U vindt ze achterin.

Inhoud

1. De vijf basisregels voor veilig betalen

We hebben de uniforme veiligheidsregels van banken in Nederland voor u omgeschreven naar vijf basisregels voor het gebruik van uw Corporate Card. Zo kunt u ze makkelijk onthouden.

Basisregel 1: Bescherm uw codes

Uw huissleutel geeft u niet aan een willekeurige voorbijganger. Doe dat ook niet met uw beveiligingscodes. Bescherm ze dus goed.

- **Onthoud uw codes**
  Kies voor beveiligingscodes/wachtwoorden niet voor een geboortejaar, een naam van een familielid of een andere code die gemakkelijk te raden is. Bent u bang om uw codes te vergeten? Noteer ze dan op zo'n manier dat ze voor anderen niet te ontcijferen zijn of probeer een ezelsbruggetje te bedenken. Zo is een zin met hoofdletters en cijfers sterk en makkelijk te onthouden. Bijvoorbeeld: 'Liever U2 dan de 6e van Beethoven!'. Als het niet past om de hele zin te gebruiken, neemt u de eerste letters van elk woord: 'LU2dd6evB!'

- Een mogelijkheid om de pincode van uw Corporate Card te onthouden is om voor elk cijfer in de pincode een woord te kiezen, waarbij het aantal letters gelijk staat aan het cijfer. Met de 4 woorden maakt u vervolgens een zin. Stel uw pincode is: 9246. U kunt dan bijvoorbeeld de zin maken: pindakaas (9) is (2) heel (4) lekker (6).

- **Laat niemand meekijken**
  Zorg dat niemand kan meekijken als u uw codes invoert. Dat kunt u doen door bijvoorbeeld het toetsenbord af te schermen met uw lichaam of met uw vrije hand.

- **Geef uw codes nooit af**
  Vraagt iemand naar uw beveiligingscodes of wachtwoorden, bijvoorbeeld voor de ING Corporate Card-portal? Geef deze dan nooit af. Uw codes zijn strikt persoonlijk. Vertel ze dus tegen niemand en onthoud dat medewerkers van ING nooit naar uw beveiligingscodes vragen: niet aan de balie, niet aan de telefoon, niet per e-mail, niet via een andere website of app dan van ING, en ook niet op andere manieren.

Basisregel 2: Bewaak uw Corporate Card

Uw portemonnee laat u niet slingeren. Doe dat ook niet met uw Corporate Card. Bewaak 'm dus goed.

- **Ga zorgvuldig met uw Corporate Card om**
  Uw Corporate Card is strikt persoonlijk. Leen deze dus niet uit. Laat uw Corporate Card nergens liggen en berg deze na gebruik direct op een vaste, veilige plaats op. Zorg ervoor dat een ander uw Corporate Card niet ongemerkt kan wegnemen.

  Geef bij voorkeur uw Corporate Card niet mee aan bijvoorbeeld een ober, maar loop zelf even mee naar de betaalterminal. Is het toch noodzakelijk om uw Corporate Card even af te geven? Controleer dan of u dezelfde kaart terugkrijgt.

  Controleer minimaal eenmaal per dag of u nog in het bezit bent van uw Corporate Card. Dit is een verplichting die ook in onze voorwaarden staat.

- **Laat u niet afleiden**
  Laat u niet afleiden als u uw Corporate Card gebruikt. Als u even niet oplet kan uw Corporate Card bijvoorbeeld makkelijk verwisseld worden voor een creditcard van dezelfde kleur. Dit noemen we de wisseltruc. Als u vermoedt dat het onveilig is om deze te gebruiken, volg dan uw gevoel en laat uw Corporate Card veilig opgeborgen.

- **Controleer regelmatig of u uw Corporate Card nog heeft**
  Wordt u op straat door een willekeurig persoon aangesproken? Liep iemand tegen u aan? Controleer daarna dan altijd of u uw Corporate Card nog heeft. Krijgt u deze niet terug nadat u hiermee betaald heeft? Neem dan direct contact met ons op (24 uur per dag, 7 dagen per week) via +31 (0)10 428 95 81 of via een van onze lokale toegangsnummers (u vindt ze achterin).

Basisregel 3: Beveilig uw apparatuur

Uw voordeur doet u op slot. Doe dat ook met de apparatuur die u gebruikt om internettransacties te verrichten met uw Corporate Card, zoals uw telefoon, tablet, desktop en laptop. Beveilig die dus goed. Dan krijgen criminelen geen kans om kwaadaardige software te installeren en bijvoorbeeld met een 'trojan' persoonlijke gegevens, zoals uw Corporate Card-gegevens te achterhalen.

- **Installeer alleen legale en bekende software**
  Zorg ervoor dat uw telefoon zo is ingesteld dat apps van onbekende bronnen niet worden toegestaan. 'Root' of 'jailbreak' uw telefoon dus niet en download alleen apps uit officiële app-stores. Installeer alleen legale software waarvan u de bron heeft gecontroleerd. Dat kunt u doen door naar de officiële website van de aanbieder te gaan. Krijgt u een onbekend softwareprogramma aangeboden? Download het programma dan niet direct, maar controleer het eerst met behulp van uw virusscanner.

- **Gebruik de nieuwste versie van de app en uw besturingssysteem**
  Zowel de ING Commercial Card app als het besturingssysteem van uw telefoon, tablet en computer worden regelmatig aangepast met meer en betere veiligheidstechnieken. Update daarom regelmatig. Stel bij voorkeur automatische updates in.

- **Stel een toegangscode in op uw apparatuur**
  Met een toegangscode voorkomt u dat anderen zeer gemakkelijk toegang hebben tot uw persoonlijke gegevens. Denk daarbij niet alleen aan uw Corporate Card-gegevens, maar ook aan uw contacten, berichten en foto's.

- **Gebruik een virusscanner, firewall en anti-spyware**
  Gebruik alleen een desktop of laptop met daarop een visrusscanner, firewall en anti-spyware om internetbetalingen te doen met uw Corporate Card. Virussen en ongevraagde programma's krijgen daardoor minder kans. Ook voor telefoons en tablets bestaan tegenwoordig virsusscanners voor extra bescherming.

- **Beveilig uw draadloze internetverbinding (wifi)**
  Zonder een beveiligde internetverbinding, verricht u geen veilige internettransacties met uw Corporate Card. Beveilig daarom uw eigen wifi met een wachtwoord. Uw internetprovider kan u daarbij helpen. Maakt u buitenshuis gebruik van een openbaar wifi-netwerk? Verricht dan bij voorkeur geen internettransacties met uw Corporate Card.

Basisregel 4: Controleer uw betalingen en afschrijvingen

Het is altijd goed om vooraf zorgvuldig na te gaan wat u precies betaalt. En kijk ook regelmatig wat er vervolgens wordt afgeschreven. Dit kan via de ING Commercial Card-portal of met de ING Commercial Card app. Deze app toont onder andere uw transacties real-time.

- **Weet wat u betaalt**
  Controleer of het bedrag dat u moet betalen juist is weergegeven op de display of - als u in het buitenland nog een handtekening op de bon moet zetten - het juiste bedrag erop staat.

Bewaar de kopie van de bon voor uw eigen administratie. Zo heeft u altijd een bewijs als het bedrag later op uw Corporate Card-afschrift niet juist is.

Zorg dat het bedrag in een vreemde valuta u achteraf niet verrast als dat wordt omgerekend naar het bedrag waarvoor u wordt belast op uw Corporate Card.

- **Hanteer de juiste volgorde**
  Vul bij een internetaankoop pas uw gegevens in, zoals creditcardnummer, vervaldatum en beveiligingscodes, als u zeker bent van uw aankoop.

- **Bekijk online uw afschrijvingen**
  Controleer uw afschrijvingen minimaal één keer per twee weken. U kunt dan beoordelen of transacties al dan niet legitiem zijn en ons bij misbruik direct op de hoogte stellen.

- **Meld schade op tijd**
  Als er schade ontstaat doordat het voor u enige tijd onmogelijk is geweest om uw Corporate Card-afschriften te controleren, kunnen wij u vragen dat aan te tonen. Schade die later wordt gemeld dan dertig dagen na de datum van uw afschrift wordt in principe niet vergoed.

Basisregel 5: Bij twijfel, bel ING

Weet u zeker of denkt u dat u het slachtoffer bent van fraude, laat dit dan direct aan ons weten. Door contact met ons op te nemen kunnen wij direct ingrijpen en eventueel verdere schade voorkomen. Wij laten bijvoorbeeld nepwebsites uit de lucht halen, zodat andere klanten niet de dupe worden van fraude.

- **Direct bellen**
  Als u fraude vermoedt, kunt u kunt ons direct bellen. Ook als uw Corporate Card, ING Commercial Card app of ING Commercial Card-portal User-ID is geblokkeerd. Of als u een verdachte e-mail heeft ontvangen en als iemand heeft geprobeerd uw Corporate Cardgegevens te ontfutselen.

- **Zorg dat wij ú ook kunnen bereiken**
  In geval van verdachte transacties willen wij u graag snel kunnen bereiken, telefonisch of via een sms-bericht. Wilt u daarom uw mobiele nummer doorgeven aan onze klantenservice? Dat kan via +31 (0)10 428 9581 of via onze lokale toegangsnummers (u vindt ze achterin).

2. Herken fraude

Ondanks alle beveiligingsmaatregelen en zorgvuldig gebruik door uzelf, blijft er kans op misbruik van uw Corporate Card. Onderstaande informatie helpt om de verschillende pogingen hiertoe te herkennen.

Fraude via uw Corporate Card

- **Skimming**
  Een bekende vorm van fraude is skimming, het kopiëren van creditcardgegevens die op de magneetstrip staan. De afgelopen jaren zijn er verschillende maatregelen tegen skimming getroffen. Daardoor komt deze vorm van fraude steeds minder voor.

- **Diefstal, wisseltrucs en afleidingsmanoeuvres**
  Nog steeds komt het voor dat dat Corporate Cards worden verwisseld of gestolen en beveiligingscodes worden afgekeken terwijl deze worden ingetoetst. Ook worden mensen afgeleid bij een geldautomaat en gaan criminelen ervandoor met het gepinde geld. De tientjestruc is hier een voorbeeld van. U wordt afgeleid met een biljet van 10 euro dat op de grond ligt, de criminelen pakken snel uw geld uit de automaat.

  Deze vormen van fraude komen vooral in winkels of bij geldautomaten voor. Pottenkijkers staan over uw schouder mee te kijken als u uw pincode intoetst en criminelen proberen u op verschillende manieren af te leiden.

Fraude via uw computer

- **Phishing**
  Bij fraude via phishing vissen criminelen via een sms of e-mail, of via een nepwebsite naar uw beveiligingscodes. Via een sms of e-mail krijgt u het verzoek op een link te klikken. Ongemerkt komt u op een nepwebsite van bijvoorbeeld de ING Commercial Card-portal, waar u gevraagd wordt in te loggen met uw beveiligingscodes. Klik dus nooit op verdachte links maar verwijder de e-mail meteen uit uw mailbox.

  Phishing-berichten kunt u als volgt herkennen:
  - In het bericht zit meestal een urgente reden voor actie verwerkt.
  - U wordt verzocht op een link te klikken. Ongemerkt komt u op een nepwebsite, waar u gevraagd wordt in te loggen met uw beveiligingscodes.
  - Het bericht lijkt vaak op een bericht van uw bank.

- **Malware**
  Malware is kwaadaardige software waarmee criminelen bijvoorbeeld uw computer op afstand kunnen bedienen. Zo kunnen ze de inloggegevens achterhalen. Op een computer zonder antivirussoftware en goede firewall kan malware eenvoudig worden geïnstalleerd. Dit gebeurt vaak zonder dat u het in de gaten heeft. Een bekend voorbeeld van kwaadaardige software is een trojan.

  Malware kunt u als volgt herkennen:
  - Soms zien internetpagina's er anders uit dan u gewend bent. Er staat bijvoorbeeld een extra invulveld voor uw telefoonnummer.
  - Een met malware besmette computer is trager en loopt vaker vast.

Fraude via de telefoon

- **Phishing**
  Ook telefonisch vissen criminelen met behulp van phishing in een telefoongesprek naar uw beveiligingscodes, zoals de pincode van uw Corporate Card, uw inloggegevens voor de ING Commercial Card-portal of andere persoonlijke gegevens. Phishing komt ook voor via sms, e-mail en nepwebsites.

  Criminelen doen zich aan de telefoon vaak voor als iemand anders. Bijvoorbeeld als een medewerker van ING of van een computer- of softwarebedrijf. Ze vertellen een geloofwaardig verhaal waarop u meestal direct moet reageren. Vervolgens vragen ze naar uw beveiligingscodes. Onthoud dat medewerkers van ING (of andere bedrijven) nooit naar uw beveiligingscodes vragen.

  Twijfelt u of u een medewerker van ING aan de telefoon heeft? Vraag dan naar zijn of haar naam en bel ons terug via het nummer achterin deze brochure. Een medewerker van ING heeft hier alle begrip voor. Wij verbinden u dan graag met hem of haar door.

  Voorbeelden van neptelefoontjes:
  - Enkele dagen na het invullen van uw creditcardgegevens in een phishing-mail belt uw bank met het verhaal dat er iets mis is met uw Corporate Card. Als u de aanwijzingen opvolgt door het verstrekken van wat laatste extra gegevens om het ‘probleem te verhelpen’, merkt u later op uw afschrift dat er fraude is gepleegd met uw Corporate Card.
  - U wordt gebeld door iemand die zich voordoet als een medewerker van een computer of softwarebedrijf. De medewerker vraagt u naar een website te gaan om software te installeren.
  - Vaak beweert men dat dit nodig is voor de veiligheid van uw computer. De software waarvan u gevraagd wordt het te installeren is malware. Als u dit installeert, zijn uw gegevens kwetsbaar die u later invult voor een internettransactie met uw Corporate Card!
  - Een persoon doet zich voor als een medewerker van ING en zegt dat hij uw gegevens moet verifiëren. Bijvoorbeeld uw gebruikersnaam en wachtwoord van de ING Commercial Card-portal.
  - Medewerkers van ING vragen u dit nooit. Geef uw codes dus niet af.

3. Wat doet ING?

In het voorgaande hebben we u heel wat adviezen en tips gegeven voor veilig betalen. Natuurlijk zorgt ING er met verschillende onzichtbare en zichtbare technieken ook voor om het gebruik van uw Corporate Card veilig te houden.

Veiligheid op de Corporate Card

- De chip op uw Corporate Card en het voorzetmondje bij de pasinvoer van een geldautomaat voorkomen skimming.
- Als u met Corporate Card afrekent, wordt tegenwoordig meestal om uw pincode gevraagd in plaats van uw handtekening. Dat is veiliger.
- Naast het creditcardnummer van uw Corporate Card heeft de kaart op de achterkant ook een CVC (Card Validation Code). Deze drie cijfercode geldt als een extra controle.

Veiligheid bij betalingen

- **SMS Security Alert**
  Bij risicovolle transacties waarvoor extra verificatie wenselijk is, krijgt u enkele seconden na de transactie via SMS een Security Alert. Via deze SMS vragen wij u om een bevestiging van de transactie. Mocht iets niet correct zijn, dan kunt u ons dat direct melden en kan uw creditcard snel worden geblokkeerd om verder misbruik te voorkomen. De SMS wordt verstuurd vanuit het nummer: +44 78 60 04 74 44.
  - Gaat het om een bekende aankoop, reageer dan op de manier zoals aangegeven in de SMS. Daarna is geen verdere actie van u nodig.
  - Is de aankoop niet bij u bekend, reageer dan op de manier zoals aangegeven in de SMS. ING zal direct uw Corporate Card blokkeren en stuurt u een tweede SMS met nadere informatie hoe verder te handelen.

  Deze service is gratis voor iedere klant met een Corporate Card. Het enige wat wij van u nodig hebben, is het juiste mobiele nummer. Bel onze klantenservice om er zeker van te zijn dat wij dat van u hebben.

  Goed om te weten is dat het niet reageren op de Security SMS geen aansprakelijkheidsgevolgen heeft bij fraude. Uw aankoop gaat wel gewoon door. Afhankelijk van de situatie kan uw kaart daarna wel (tijdelijk) geblokkeerd zijn voor een volgende aankoop.

- **Mastercard ID check**
  Internetaankopen bij bedrijven die deelnemen aan Mastercard ID check worden op de achtergrond beschermd tegen misbruik. U zult dan een scherm zien met de tekst ‘Verwerken’. In de meeste gevallen zal ING alle veiligheidscontroles op de achtergrond uitvoeren, maar bij sommige transacties zullen wij u vragen om een eenmalige code in te voeren. Deze code ontvangt u per SMS. Maak het ons en uzelf makkelijk en zorg dat wij uw mobiele nummer hebben.

- **Blokkeren van de Card**
  Bij (zeer) verdachte situaties kan ING besluiten uw Corporate Card preventief te blokkeren. U wordt hiervan altijd zo snel mogelijk op de hoogte gesteld via de telefoon, per sms of per brief. Mocht u merken dat uw transactie niet lukt, neem dan direct contact met ons op.

4. Fraude, wat nu?

ING doet er alles aan om te voorkomen dat u slachtoffer wordt van fraude. En als u de adviezen en tips in deze brochure zoveel mogelijk probeert toe te passen, krijgen criminelen weinig kans om fraude te plegen met uw Corporate Card. Mocht u toch slachtoffer zijn geworden van fraude, dan brengen wij dit graag en snel voor u in orde. Handel daarom als volgt:

Fraude melden

- **Zo snel mogelijk**
  Meld (een vermoeden van) fraude zo snel mogelijk telefonisch bij ons. Dit kan 24 uur per dag, 7 dagen per week. Doe dit in ieder geval uiterlijk 30 dagen na de datum van uw afschrift (digitale of papieren versie). Door een snelle melding kunnen wij meestal voorkomen dat het bedrag bij u of bij het bedrijf wordt geïncasseerd. Dit voorkomt onvoorziene financiële gevolgen voor u of het bedrijf. Ook kunnen wij u dan direct een nieuwe Corporate Card toezenden.

- **Fraudeformulier**
  Na de telefonische melding sturen wij u een fraudeformulier per post of, indien u dat wenst, per e-mail. Onze voorwaarde: stuur het formulier uiterlijk binnen 14 dagen retour. Hoe sneller u de formulieren ingevuld retourneert, des te eerder uw fraudemelding kan worden afgehandeld. Soms kan het noodzakelijk zijn dat wij extra informatie van u nodig hebben als de winkelier waar het misbruik heeft plaatsgevonden hierom vraagt.

- **Proces-verbaal**
  Indien er fraude is verricht met uw Corporate Card terwijl deze verloren, gestolen, niet ontvangen of niet door u is aangevraagd, moet u bij het fraudeformulier een door de politie opgesteld proces-verbaal bijvoegen.

Schadevergoeding

- **Ons beleid**
  Als u niets te verwijten valt wordt fraude altijd vergoed. Tijdens het telefoongesprek zal onze medewerker er zoveel mogelijk voor zorgen dat u hiervoor niet wordt belast. In sommige gevallen (bijvoorbeeld als de incasso-opdracht al door ons is verstuurd) kunnen wij dit echter niet voorkomen. Wij zullen altijd in overleg met u de situatie bespreken, zodat de vergoeding zo snel mogelijk wordt geregeld.

  Op basis van uw schriftelijke verklaring en het door ons gevoerde onderzoek naar het misbruik van uw Corporate Card zal de vergoeding definitief worden. Wij laten u dat altijd schriftelijk weten.

5. Begrippenlijst

A

Anti-spyware
Anti-spyware is een van de hulpmiddelen waarmee u uw computer beveiligt. Deze software zorgt ervoor dat er geen ongevraagde programma's worden geïnstalleerd die uw persoonlijke gegevens kunnen verspreiden.

Antivirussoftware
Zie 'Virusscanner'

B

Besturingssysteem
Een computer, tablet of smart telefoon kunnen alleen maar juist functioneren als daar software op staat. Software die geschreven is om deze apparaten juist te laten werken wordt een besturingssysteem genoemd.

Botnet
Een botnet is een netwerk van heel veel computers, dat besmet is door een Trojan of virus. Hierdoor wordt de computer als het ware een robot, die zelfstandig en automatisch werk kan uitvoeren. De geïnfecteerde computers kunnen overal staan. Ook uw computer kan er deel van uitmaken. Criminelen kunnen vervolgens al deze computers in één keer een opdracht geven. De computers worden dan bijvoorbeeld gebruikt voor het verzenden van phishing e-mails. Of om uw Corporate Card-gegevens te onderscheppen.

Browser
Een browser is een computerprogramma waarmee u op internet websites kunt bekijken. Bekende browsers zijn Internet Explorer, Chrome, Firefox en Safari

C

Commercial Card-portal
Met de ING Commercial card-portal kunt u uw Corporate Card-afschriften digitaal terugvinden tot 12 maanden terug.

Computervirus
Zie 'Virus'

Cookie
Een cookie is een klein bestandje dat door een website op uw computer wordt gezet. Hiermee wordt uw surfgedrag opgeslagen. Veel webwinkels maken gebruik van cookies, zodat uw gegevens bij een volgend bezoek al ingevuld zijn.

Commercial Card app
De Commercial Card app is de officiële app voor uw Corporate Card. U kunt hiermee uw transacties direct bekijken tot maximaal 12 maanden terug. Zoek voor de download in de Apple App Store of in Google Play (Android) op 'ING Commercial Card app'.

CVC
CVC staat voor Card Validation Code. Het is een 3-cijferige veiligheidscode, die op de achterzijde van uw Corporate Card rechts naast het handtekeningveld staat. Hiernaar kan worden gevraagd als u een internet betaling verricht met uw Corporate Card.

Cybercrime
Cybercrime is criminaliteit via internet. Zo versturen criminelen e-mails waarin zij naar uw inloggegevens en/of gegevens van creditcards vragen (phishing) en maken zij websites die sterk op ING-websites lijken. Ook proberen zij uw persoonlijke gegevens van uw computer te halen via een virus dat ze meesturen met een ander programma (een zogenaamde Trojan).

D

DDoS-aanval
Tijdens een DDoS-aanval wordt een internetsite bestookt met dataverkeer. Dit ongewenste dataverkeer wordt tegengehouden door de firewall. Op het moment dat het ongewenst dataverkeer extreem groot wordt, is de firewall zo druk met het tegenhouden van dit ongewenste verkeer dat ook de gewenste bezoekers er niet meer doorheen komen. ING hanteert een zeer hoog niveau van veiligheidsmaatregelen. Deze maatregelen zijn er op gericht het ongewenste dataverkeer van het goede dataverkeer te scheiden.

Detectie
Detectie is het opsporen van verdachte handelingen. ING heeft een team van experts in huis dat zich dagelijks bezig houdt met de veiligheid van betalen. Wij analyseren voortdurend verdachte transacties en handelingen. En ondernemen actie waar dat nodig is. ING werkt nauw samen met politie, overheid en andere partijen, nationaal en internationaal. Op die manier kunnen we u zo snel en goed mogelijk informeren.

E

EMV-chip
De EMV-chip is sinds enkele jaren de chip op uw Corporate Card. Hierdoor kunt u nu bijvoorbeeld in winkels met een pincode betalen met uw Corporate Card. De EMV-chip is een internationale standaard die wereldwijd wordt gebruikt. De chip vermindert de creditcardfraude in winkels. U haalt uw Corporate Card dus niet meer langs een magneetstriplezer, maar steekt de Corporate Card in de betaalautomaat. Op deze manier wordt de EMV-chip gelezen

Extensie
Een extensie is een extra applicatie voor uw browser die u zelf kunt downloaden. Hiermee is het mogelijk nieuwe functies aan uw browser toe te voegen. Voorbeelden van extensies zijn Adobe Reader voor het lezen van pdf-files en Flash voor het bekijken van YouTube-video's.

F

Firewall
Een firewall is een van de hulpmiddelen waarmee uw computer beveiligd kan worden. Deze software helpt te voorkomen dat anderen toegang krijgen tot uw computer als deze is aangesloten op internet of een computernetwerk. Een firewall controleert inkomend en uitgaand internetverkeer. U krijgt een waarschuwing bij twijfelachtige gegevensuitwisseling

Fraude
Op verschillende manieren kunt u het slachtoffer worden van fraude. Deze brochure is opgesteld om u te informeren over fraude.

G

Geldezel
Een geldezel stelt zijn of haar bankrekening beschikbaar voor criminele activiteiten. Criminelen storten geld op de bankrekening, sluizen het door naar andere rekeningen of nemen het contant op. Op die manier verbergen ze gestolen geld voor politie en justitie.

I

Identiteitsfraude
Identiteitsfraude houdt in dat criminelen uw persoonlijke en financiële gegevens verzamelen en daarvan later misbruik maken. Ingeslepen gewoontes, zoals het argeloos weggooien van financiële informatie, afschriften van uw Corporate Card, een handtekening of een kopie van uw identiteitsbewijs, kunnen identiteitsfraude in de hand werken. Maar ook via phishing en social engineering bemachtigen criminelen persoonlijke gegevens. Vervolgens kan een crimineel in uw naam bijvoorbeeld een aanvraag voor een creditcard indienen.

Internetcrimineel
Internetcriminelen houden zich bezig met criminaliteit op internet. Zo versturen zij e-mails, waarin zij naar uw inloggegevens en/of gegevens van creditcards vragen (phishing). Ook maken internetcriminelen websites die sterk op website van ING lijken. Of zij proberen uw persoonlijke gegevens van uw computer te halen via een virus dat ze meesturen met een ander programma (een Trojan).

J

Jailbreaken
Jailbreaken is het omzeilen van een beveiligingsmaatregel van het besturingssysteem van een iPhone, iPod touch of iPad. Door het apparaat te jailbreaken, kan de gebruiker bijvoorbeeld apps installeren die niet door Apple zijn goedgekeurd. Hierdoor is een dergelijk toestel vatbaarder voor bijvoorbeeld virussen en malware.

K

Katvanger
Zie ‘Geldezel’

M

Malware
Malware is een verzamelnaam voor kwaadaardige en/of schadelijke software. Het woord is een samenvoeging van het Engelse ‘malicious software’ (kwaadwillende software). Malware wordt speciaal ontworpen om een computer te infiltreren zonder dat u daar maar zelfs van op de hoogte hoeft te zijn. Malware kan uw computer bijvoorbeeld binnenkomen via e-mail of afbeeldingen op websites.

MasterCard ID check
Zie hoofdstuk ‘Wat doet ING?

Money mule
Zie ‘Geldezel’

N

NCSC
Nationaal Cyber Security Centrum. Samenwerking van overheden en bedrijven. Missie: Het NCSC draagt bij aan het gezamenlijk vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein, en daarmee aan een veilige, open en stabiele informatiesamenleving door het leveren van inzicht en het bieden van handelingsperspectief.

P

Phishing
Phishing is het 'vissen' naar uw persoonlijke gegevens door criminelen. Met één doel: informatie te verkrijgen over uw Corporate Card en daarmee transacties te verrichten. Dat kan via e-mail, telefoon of website gebeuren. U wordt bijvoorbeeld verzocht op een link in een nep e-mail te klikken. Het bericht lijkt bedrieglijk echt op dat van de ING. Ongemerkt komt u op een nepwebsite waarin uw Corporate Card gegevens doorgeeft. Zonder dat u er erg in heeft, kunnen criminelen nu transacties verrichten met uw Corporate Card.

Preventief blokkeren
Om het betaalverkeer veilig te houden, neemt ING in verdachte situaties direct maatregelen. Om uw Corporate Card te beschermen, kunnen wij overgaan tot preventief blokkeren. Bijvoorbeeld als we vermoeden dat uw Corporate Card geskimd is. Dan blokkeren we uw creditcard en proberen wij direct contact met u op te nemen.

R

Ransomware
Ransomware is een chantagemethode door middel van malware. Ransomware is een programma dat uw computer blokkeert en vervolgens geld vraagt om de computer weer te 'bevrijden'. Betalingen (bijvoorbeeld met uw Corporate Card) zorgen alleen niet voor een 'bevrijding' van uw computer, omdat de criminelen alleen op uw geld uit zijn

Rooten
Rooten is het omzeilen van een beveiligingsmaatregel van het besturingssysteem van een Android-telefoon of Android-tablet. Door het apparaat te rooten, kan de gebruiker bijvoorbeeld apps installeren die niet voor de Android Market zijn goedgekeurd. Hierdoor is een dergelijk toestel vatbaarder voor bijvoorbeeld virussen en malware.

S

Security Alert Service
Zie hoofdstuk 'Wat doet ING?

Skimming
Skimming is het kopiëren van uw Corporate Card gegevens door het plaatsen van een extra kaartleesapparaatje op de pasinvoer van een geld- of betaalautomaat. Criminelen kijken vervolgens uw persoonlijke pincode af, waarna zij met de geskimde gegevens geld opnemen. Door het plaatsen van speciale voorzetmondjes op de pasinvoer van geldautomaten probeert de ING te voorkomen dat criminelen kaartlezers kunnen plaatsen. Daarnaast worden winkeliers aangemoedigd periodiek te controleren of criminelen misschien hun betaalautomaat hebben gemanipuleerd.

Smishing
Smishing is phishing via sms. Zie ‘Phishing’

Social engineering
Bij social engineering proberen criminelen vertrouwelijke informatie van u te ontfutselen. Ze misbruiken menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst en onwetendheid. Social engineering kent veel vormen. Van valse websites tot phishing e-mails en van telefoongesprekken tot persoonlijk contact aan de deur. Criminelen laten u een bepaalde handeling uitvoeren, zoals het invullen van persoonlijke gegevens, beveiligingscodes of creditcardgegevens, het indrukken van een knop of het installeren van malware.

Spyware
Spyware is software, die (onopgemerkt) op een computer wordt geïnstalleerd. Hiermee kunnen gegevens over de gebruiker verzameld en doorgestuurd worden naar derden.

T

Tientjestruc
Criminelen proberen iemand die geld staat op te nemen bij een automaat af te leiden door een tientje op de grond te gooien. Ze zeggen dan dat je het hebt laten vallen, maar stelen ondertussen je geld uit de automaat.

Toegangscode
Op uw computer of telefoon/tablet/computer kunt u zelf een code instellen zodat anderen niet zomaar gebruik kunnen maken van deze apparatuur.

Trojan (of Trojaans paard)
Trojan is afgeleid van Trojan horse (Trojaans paard). Een Trojan is een programma, dat ‘vermomd’ als een onschuldig bestand ongemerkt op uw computer wordt geïnstalleerd. Hiermee kunnen criminelen op afstand in uw computer. Zonder dat u het zelf in de gaten heeft. Via Trojans kunnen zij bijvoorbeeld uw gebruikersnaam en wachtwoord voor de ING Commercial Card-portal achterhalen.

V

Valse e-mail
Zie ‘Phishing’

Veiligheidsexpert
Wij hebben een team van veiligheidsexperts in huis dat voortdurend verdachte transacties en handelingen analyseert. We ondernemen actie waar dat nodig is. ING werkt nauw samen met politie, overheid en partijen als de Nederlandse Vereniging van Banken.

Virus
Een virus is een vorm van schadelijke software. Virussen kunnen ernstige schade aanrichten in uw computer, waardoor (vertrouwelijke) informatie wordt gewist. Ook kunnen criminelen met behulp van een virus meekijken op een computer en zo uw gebruikersnaam en wachtwoord achterhalen.

Virusscanner
Een virusscanner is een van de hulpmiddelen waarmee uw computer beveiligd kan worden. Deze software controleert of uw computer virussen bevat en kan deze virussen verwijderen.

Voorzetmondje
Een voorzetmondje is een voorzetstukje op de pasinvoer van een geldautomaat. Hierdoor kunnen criminelen geen kaartlezer plaatsen die creditcardgegevens kopieert. Het kopiëren van creditcardgegevens wordt skimming genoemd. Per type geldautomaat kan het voorzetmondje verschillen. Op het scherm van de geldautomaat wordt het juiste mondje getoond.

W

Wachtwoord
Bij veilig bankieren hoort een sterk wachtwoord. Een wachtwoord is sterk als het niet te raden is en moeilijk te kraken. Gebruik dus een sterke wachtwoorden voor al uw online omgevingen.

WiFi
WiFi is de Engelse afkorting voor een draadloos netwerk. Via het draadloze netwerk kunt u op internet komen.

Worm
Een worm probeert zichzelf te verspreiden over netwerken. Een worm verplaatst zich automatisch zoals in een kettingreactie. Meestal gebeurt dit via e-mailadressen die op een geïnfecteerde computer worden aangetroffen.

6. Belangrijke telefoonnummers

Bij (een vermoeden van) fraude kunt u ons 24 uur per dag, 7 dagen per week bereiken via

+31 (0)10 428 95 81

of via onze lokale toegangsnummers. Deze nummers kunt u vinden op:

www.ingwb.com/cardcontact

Aarzel niet, wij staan voor u klaar!

ING Bank N.V. is statutair gevestigd aan Bijlmerplein 888, 1102 MG Amsterdam, handelsregister nr. 33031431 in Amsterdam. ING Bank N.V. is geregistreerd bij De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM) in het Register Kredietinstellingen en Financiële Instellingen. Ook staat ING Bank N.V. onder het toezicht van de Autoriteit Consument & Markt (ACM). Informatie over het toezicht op ING Bank N.V. kan worden verkregen bij DNB (www.dnb.nl), de AFM (www.afm.nl) of de ACM (www.acm.nl).

Onder '(de) ING' of 'de bank' wordt in deze publicatie verstaan: 'ING Bank N.V.'