Voorkom fraude, wees alert !

Een veilig gebruik van creditcards:

1. **Geef nooit de gegevens van uw creditcard aan vreemden.**

   Geef nooit de gegevens van uw creditcard of andere persoonlijke of financiële informatie aan onbekenden die u ongevraagd op straat, telefonisch, schriftelijk dan wel per email benaderen. Zo zal een bankmedewerker of politiefunctionaris ook nooit naar uw pincode informeren.

   Gebruikte trucs om creditcardgegevens te ontfutselen:

   - Er wordt u een orderbevestiging toegezonden van producten die u niet heeft besteld. U wordt gevraagd uw creditcardgegevens door te geven om de bestelling te bevestigen of ongedaan te maken
   - Er wordt verteld dat u een prijs hebt gewonnen. Het enige dat u hiervoor moet doen is even het nummer van uw creditcard doorgeven.
   - De klantgegevens van een organisatie worden bijgewerkt. U wordt gevraagd even uw creditcardgegevens in te vullen, zodat alle informatie weer up-to-date is

   Reageer **niet** op dit soort e-mails of telefoontjes en geef nooit uw persoonlijke financiële gegevens door. Geef alleen uw creditcardgegevens door, als u zelf bewust een order plaatst. Uw pincode is strikt persoonlijk, geef deze dus **nooit** aan derden! Zolang u niet reageert op dit soort oproepen, is er niets aan de hand. De criminelen beschikken dan immers niet over uw creditcardgegevens.

   Neem in geval van twijfel contact op met uw bank of creditcardmaatschappij.

2. **Phishing**

   Phishing is het onrechtmatig verzamelen van financiële gegevens via een (*valse)* e-mail of website. Let daarom op de volgende punten:

   - Gerenommeerde organisaties, zoals banken, creditcardmaatschappijen en andere legitieme bedrijven vragen nooit per e-mail om persoonlijke gegevens, wachtwoorden en creditcardgegevens
   - Een phishing e-mail is vaak onpersoonlijk opgesteld. De aanhef luidt 'Beste klant', 'Beste bedrijfsnaam klant', 'Beste gebruiker', of er staat helemaal geen aanhef
   - Pogingen tot phishing gericht op Nederlandse klanten, zijn vaak in het Engels opgesteld.
   - Wees alert op e-mails afkomstig van onbekende partijen.
   - Phishing e-mails spelen vaak in op uw angst opgelicht te worden of uw account kwijt te raken. Het gaat vaak om een 'dringende reden' zo snel mogelijk te reageren, omdat er een beveiligingsprobleem zou zijn, uw account dreigt te verlopen of administratieve kosten dreigen op te lopen

   Meer informatie betreffende phishing vindt u op www.digibewust.nl

3. Geld opnemen / Betalen

Houd uw pincode privé en scherm tijdens het intoetsen van uw pincode bij een betaal- of geldautomaat het toetsenbord zorgvuldig met uw hand of lichaam af. Ook voor het betalen met een creditcard heeft u in steeds meer situaties de bijbehorende pincode nodig.

Laat persoonlijke gegevens zoals transactiebonnetjes etc. niet slingeren rond geld-automaten of in openbare gelegenheden.

Loop even mee naar de kassa wanneer u betaalt. Dan hoeft u uw kaart niet uit het oog te verliezen.

Controleer het bedrag voordat u de transactiebon tekent. Bewaar vervolgens een kopie van de transactiebon en neem deze mee naar huis. Op deze manier kunt u de rekeningoverzichten controleren.

4. Verlies of diefstal

Ga zorgvuldig om met uw creditcard, bewaar hem bij voorbeeld in uw portefeuille en niet los in broek- of jaszak. Uw creditcard is geld waard!

Laat uw bankpassen en creditcards bij verlies of diefstal direct blokkeren. Noteer de telefoonnummers voor het blokkeren van bankpassen en creditcards in uw agenda of zet ze in uw mobiele telefoon. Snel blokkeren voorkomt financiële schade.

U vermoedt misbruik van uw card of cardgegevens ? Neem dan zo snel mogelijk contact op met uw bank of creditcardmaatschappij waar 7 dagen per week, 24 uur van de dag mensen beschikbaar zijn om u in deze te helpen. Fraude kan ook de kaarthouder geld kosten, bijvoorbeeld een bedrag aan eigen risico.

Controleer regelmatig of u nog in het bezit bent van uw bankpassen en creditcards.

Doe bij daadwerkelijk financiële schade door frauduleus gebruik van uw creditcard aangifte bij uw lokale politiebureau.

Zorg dat uw brievenbus is beveiligd tegen diefstal (hengelen) van uw poststukken

5. Veilig gebruik creditcard op internet

Zorg dat uw eigen computer voldoende beveiligd is, ook tegen virussen en spyware.

Wanneer u op deze wijze wilt betalen, kan er gevraagd worden naar uw CVC (Card Validation Code) of CVV (Card Verification Value). Deze codes bestaan uit de laatste drie cijfers die u vindt op de handtekeningstrook aan de achterzijde van uw creditcard.

Maak op internet alleen gebruik van beveiligde sites om uw persoonlijke en/of financiële gegevens te versturen. Deze sites zijn te herkennen aan het icoontje met het slotje dan wel een sleutel. Indien je hierop klikt, dan kun je zien aan wie het certificaat is verstrekt.

Sites met meer informatie;

www.americanexpress.nl
www.digibewust.nl
www.dinersclub.nl
www.mastercard.nl
www.vanstripnaarchip.nl
www.veiligbankieren.nl
www.visa.nl

Kijk ook op de site van uw eigen bank of creditcardmaatschappij.

Een veilige acceptatie van creditcards:

1. De *toonbank*situatie

Verplicht voorgeschreven controles;

- Controleer de echtheidskenmerken van de aangeboden creditcard en bekijk de specifieke kenmerken van de kaart onder UV-licht. Voorlichtingsmateriaal waarin deze kenmerken zijn opgenomen kan worden aangevraagd bij uw creditcardmaatschappij.
- Controleer of de handtekening op de creditcard overeenkomt met de handtekening op de transactiebon.
- Controleer aan de hand van de vervaldatum op de creditcard of het een geldige kaart betreft.
- Controleer altijd of de laatste vier cijfers van het kaartnummer op de creditcard overeenkomen met die van het kaartnummer op de transactiebon.

Het niet opvolgen van bovenvermelde controles zou in geval van fraude kunnen leiden tot een aansprakelijkheidsstelling voor de geleden schade.

Beoordeel voorts de aanbieder van de kaart en de omstandigheden waaronder de kaart wordt aangeboden. (Zie onder 2) Wees alert op fraude.

Vraag in geval van twijfel om een legitimatiebewijs aan de aanbieder om vast te stellen dat de combinatie van kaart en aanbieder overeenstemt.

Bij blijvende twijfel houdt, indien de situatie dit toelaat, de creditcard in uw bezit en bel de autorisatieafdeling van uw creditcardmaatschappij voor een code 10-gesprek.

2. Herkenning van een mogelijke fraudeur

Een klant met frauduleuze bedoelingen is mogelijk te herkennen aan zijn of haar gedrag. Kenmerkend gedrag in deze:

- De klant koopt duurdere artikelen, laat zich nauwelijks voorlichten en maakt (te) snel een keuze.
- De klant past uitgezochte kleding niet of gehaast en wenst deze ook niet te laten vermaken.
- De klant verschijnt vlak voor sluitingstijd in de winkel en koopt voor een aanzienlijk bedrag.
- De klant draagt zijn creditcard los bij zich (niet in portefeuille of portemonnee) en heeft veelal direct een andere creditcard beschikbaar in het geval van een afwijzing.
- De klant gedraagt zich anders dan andere klanten, is zichtbaar nerveus en probeert de aankoop snel af te wikkelen.
- De klant probeert u af te leiden door bijvoorbeeld veel te praten.
- De klant zet onnatuurlijk precies zijn handtekening en doet daar langer over dan normaal.
- De klant komt snel na de aankoop terug en verricht nogmaals (duurdere) aankopen.
- De klant probeert recente aankopen weer in te ruilen en in contanten om te zetten.

3. De internetsituatie

Creditcards zijn een zeer gewild betaalmiddel op internet. Helaas komt misbruik in deze omgeving voor. Om fraude te voorkomen is het raadzaam te letten op een aantal hieronder weergegeven zaken doch de belangrijkste regel: **Gebruik uw gezond verstand.**

Let op vreemde bestellingen. Houdt bestellingen goed in de gaten, ook over langere periodes. Zijn er vreemde aantallen besteld? Is het afleveradres ongebruikelijk? Neem dan het zekere voor het onzekere en controleer of de bestelling in orde is. Voorbeelden van ongebruikelijke bestellingen zijn;

* bestellingen vanaf naastgelegen huisnummers;

* bestellingen vanaf verschillende adressen via hetzelfde e-mailadres;

* bestellingen vanuit geografische gebieden die niet logisch zijn omdat de producten moeilijk te versturen zijn of omdat de producten in dat gebied goedkoper zijn;

* bestellingen die snel achter elkaar worden geplaatst met verschillende creditcards;

* bestellingen van meerdere dezelfde artikelen op één adres terwijl dit onlogisch is qua gebruik binnen één huishouden/gezin.

Analyseer de bestellingen en vergelijk de verschillende orders/situaties met elkaar. Verplaats u in de situatie, is een bepaalde bestelling logisch als je een welwillende en te goeder trouwe consument bent?

Vraag om orderbevestiging per fax of telefoon
Zeker bij hoge bedragen adviseren wij u extra controles uit te voeren. Zoals bij voorbeeld vragen om een orderbevestiging per fax. Of u belt even met de klant op een vaste telefoonlijn. Controleer het telefoonnummer aan de hand van het telefoonboek. U kunt opgave van telefoonnummer en e-mailadres verplicht stellen. Wees extra alert bij de opgave van 06-nummers en gratis e-mailadressen (zoals Hotmail).

Vraag de Card Validation Code / Card Verification Value
De driecijferige Card Validation Code (CVC) is een extra controlemiddel naast onder meer de vervaldatum en het kaartnummer. Ook hiervan kunt u de opgave verplicht stellen.

Vraag bij aflevering om een handtekening

Om zeker te zijn dat u de bestelling op het juiste adres aflevert, kunt u bij bezorging om een handtekening vragen. Lever alleen af aan de geadresseerde. Bezorg niets bij de buren als de geadresseerde niet aanwezig is. Wij ontraden u te bezorgen op postbusnummers. Informeer eventueel bij uw vervoerder hoe de goederen in ontvangst zijn genomen.

Let op bij bepaalde producten
Elektronica (gsm's, camera's, hardware, etc), video- en muziekcontent, software, dure merk- of erotische artikelen zijn voorbeelden van producten die via internet een hoger risico lopen op frauduleuze bestellingen. Extra aandacht is daarom geboden.

Informeer bij uw Payment Service Provider (PSP) welke service of middelen op het gebied van fraudepreventie zij bieden. Uw PSP kan vaak meerdere controles uitvoeren op gegevens waar u als ondernemer niet over beschikt.

Samen werken aan veiligheid

De creditcardmaatschappijen helpen u graag om fraude te voorkomen en werken daarom voortdurend aan nieuwe methoden om misbruik van creditcards onmogelijk te maken. Eén van de ontwikkelingen in dit verband is de introduktie van Verified by Visa of MasterCard® SecureCode™. Informeer bij uw Payment Service Provider of Verified by Visa en/of MasterCard SecureCode ook bij u mogelijk is en op welke andere manieren zij u kunnen helpen uw internetbetalingen nóg veiliger te maken.

Sites met meer informatie;

www.americanexpress.nl
www.digibewust.nl
www.dinersclub.nl
www.mastercard.nl
www.vanstripnaarchip.nl
www.veiligbankieren.nl
www.visa.nl

Kijk ook op de site van uw eigen bank of creditcardmaatschappij.