

## Veilig internet

Met onderstaande algemene informatie hopen wij eventuele zorgen over de veiligheid van online-transacties weg te nemen. Indien u meer specifieke vragen hebt, dan verzoeken wij u contact met ons op te nemen.

Veiligheid staat bij Mandema voorop. Mandema stelt al het mogelijk in het werk om te voorzien in een optimale beveiliging van uw gegevens. Dat geldt ook als u gebruikt maakt van Mandema websites via het Internet.

### Mandema websites zijn in te delen in twee categorieën:

1. Mandema websites met vrij toegankelijke informatie (hiervoor is geen gebruikersnaam + wachtwoord nodig).
2. Mandema websites met de mogelijkheid informatie uit te wisselen tussen u als klant en Mandema en Partners B.V. (hiervoor is wel een gebruikersnaam + wachtwoord nodig).

Wij passen vergaande beveiligingsmethoden en –technieken toe om het bezoek aan en eventueel het gebruik van onze websites zo veilig mogelijk te laten zijn.

Bescherming van de gegevens van onze klanten is voor ons onderdeel van een goede bedrijfsvoering. Hoezeer wij ons ook inspannen, het internet brengt risico's met zich mee. Snel ontwikkelende technieken en het feit dat internet zeer moeilijk controleerbaar is, maken het bijvoorbeeld lastig internet waterdicht te beveiligen. Natuurlijk volgen wij de snelle technische ontwikkelingen en past indien nodig de beveiliging aan.

Om internetgebruik zo veilig mogelijk te laten zijn is het noodzakelijk dat wij met u als klant samenwerkt. Dit doen we door een aantal afspraken te maken.

### Wat doet Mandema & Partners?

- Mandema websites zijn duidelijk herkenbaar en het internetadres (de url) bevat geen spelfouten, dus [www.mandema.nl](http://www.mandema.nl) is goed, [www.madema.nl](http://www.madema.nl) niet.
- Mandema websites waarmee informatie wordt uitgewisseld voorzien in een beveiligde verbinding tussen de Mandema website en uw PC.
- Mandema websites waarmee informatie wordt uitgewisseld, zijn alleen toegankelijk, als u uw persoonlijke gebruikersnaam en wachtwoord invoert.
- Mandema websites waarmee belangrijke en persoonlijke informatie wordt uitgewisseld (bv. financiële transacties, medische gegevens) werken alleen als u een geheime code invoert.
- Mandema websites worden getest op de beveiliging ervan (hackerstesten).
- Mandema zal NOOIT vragen naar uw gebruikersnaam, wachtwoord of geheime codes. NOOIT, dus niet op de site en ook niet via e-mail, telefoon of op welke andere manier dan ook! Deze gegevens zijn persoonlijk en geven toegang tot informatie die alleen voor u van belang is. Het is uw sleutel en die mag u nooit aan anderen geven. Doet u dat toch, dan geeft u daarmee zelf toegang en bent u zelf aansprakelijk voor eventuele gevolgen.
- Mandema zal u nooit via een e-mail doorverwijzen naar een website waar u beveiligde informatie moet invoeren.
- E-mails van Mandema zijn altijd op naam gesteld.

### Wat kunt u zelf doen?

- Controleer de beveiligde verbinding. Het internetadres (URL) begint met <https://>. Ook verschijnt er een icoon met een gesloten hangslotje op de onderste balk van uw internetbrowser. Als u klikt op het icoontje met het hangslot dan verschijnt er een beveiligingscertificaat. Dit certificaat laat zien wie de eigenaar van de site is. Controleer of de gegevens en de rechtsgeldigheid kloppen.

- Reageer niet op e-mails en dergelijke, hoe echt ze ook lijken, waarin om uw gebruikersnaam en/of wachtwoord wordt gevraagd.
- Ga zorgvuldig met uw persoonlijke gebruikersnaam, wachtwoord en uw geheime codes om (of het apparaat dat deze code genereert). Schrijf nooit uw persoonlijke informatie gegevens op in voor anderen toegankelijke media en noem ze niet in een e-mail.
- Gebruik de nieuwste versie van uw internetbrowser en bij voorkeur ook uw besturingssysteem (windows, apple, linux, etc.) en actualiseer deze regelmatig.
- Bescherm uw PC met speciale software tegen virussen en spyware en actualiseer deze regelmatig.
- Maak gebruik van een zogenaamde firewall.
- Pas op voor spam: Gebruik een spam-filter om te voorkomen dat u dergelijke berichten ziet. Beantwoord nooit een spam-bericht. Dan weet men uw e-mailadres en neemt de hoeveelheid spam alleen maar toe. Wanneer u spam-berichten leest, realiseer u dan: wanneer een aanbieding te mooi lijkt om waar te zijn, dan is het dat waarschijnlijk ook.

Als u zich aan deze voor u geldende afspraken houdt is "veilig internetgebruik" bijna vanzelfsprekend en voorkomt u dat criminelen misbruik kunnen maken van de voor u belangrijke en persoonlijke gegevens.

Als bepaalde criminelen echt tot doel hebben uw persoonlijke en financiële gegevens te achterhalen en te misbruiken zullen zij zeer slim te werk gaan. Daarom is het tot slot goed om te weten welke vormen van internet criminaliteit er bestaan.

## **Wij onderscheiden twee vormen van internet criminaliteit.**

### **1. Phishing**

Phishing is oplichting via Internet. Fraudeurs proberen door misleiding persoonlijke informatie van u te bemachtigen. Dit gebeurt via misleidende e-mails die van bekende bedrijven en banken afkomstig lijken te zijn, of via 'imitatie'-websites. Sites die lijken op betrouwbare sites van bekende bedrijven en banken doordat ze gebruik maken van bedrijfslogo's en de inhoud van de e-mail sterk lijkt op de communicatie-uitingen van het geïmiteerde bedrijf.

Fraudeurs vragen u dan in bijvoorbeeld een e-mail om uw gebruikersnaam en wachtwoord, geheime codes, pinpas- en/of creditcardinformatie of sofinummer.

Soms worden trucs toegepast om u snel te laten reageren: men dringt er dan op aan dat u zo snel mogelijk op een meegestuurde link klikt (die heel erg lijkt op die van het geïmiteerde bedrijf), omdat anders bijvoorbeeld uw account vervalft, of u geen gebruik meer kunt maken van een speciale actie. Als u dan op deze meegestuurde link klikt komt u op een 'imitatie'-website. Op deze website vraagt men u persoonlijke gegevens in te voeren. Met deze gegevens zullen de fraudeurs dan op de 'echte' site proberen misbruik te maken van deze gegevens, bijvoorbeeld door namens u transacties uit te voeren.

### **2. Pharming**

Net als bij phishing is het doel van pharming achter uw gevoelige (persoonlijke) gegevens te komen, zoals een wachtwoord, of het nummer van uw creditcard.

Dit werkt niet via een e-mail, maar direct via een speciaal daarvoor opgezette valse website, waarnaar u ongemerkt wordt doorgesluisd. Deze website lijkt net als bij phishing exact op de officiële versie ervan. Verschil is dat, ook als u een correct internetadres (URL) invoert, u kunt worden doorgesluisd naar een perfect nagebouwde valse website. Het internetadres wordt als het ware 'gekaapt' door de kwaadwillenden. Ook hier geldt dus dat u zelf altijd waakzaam moet zijn!