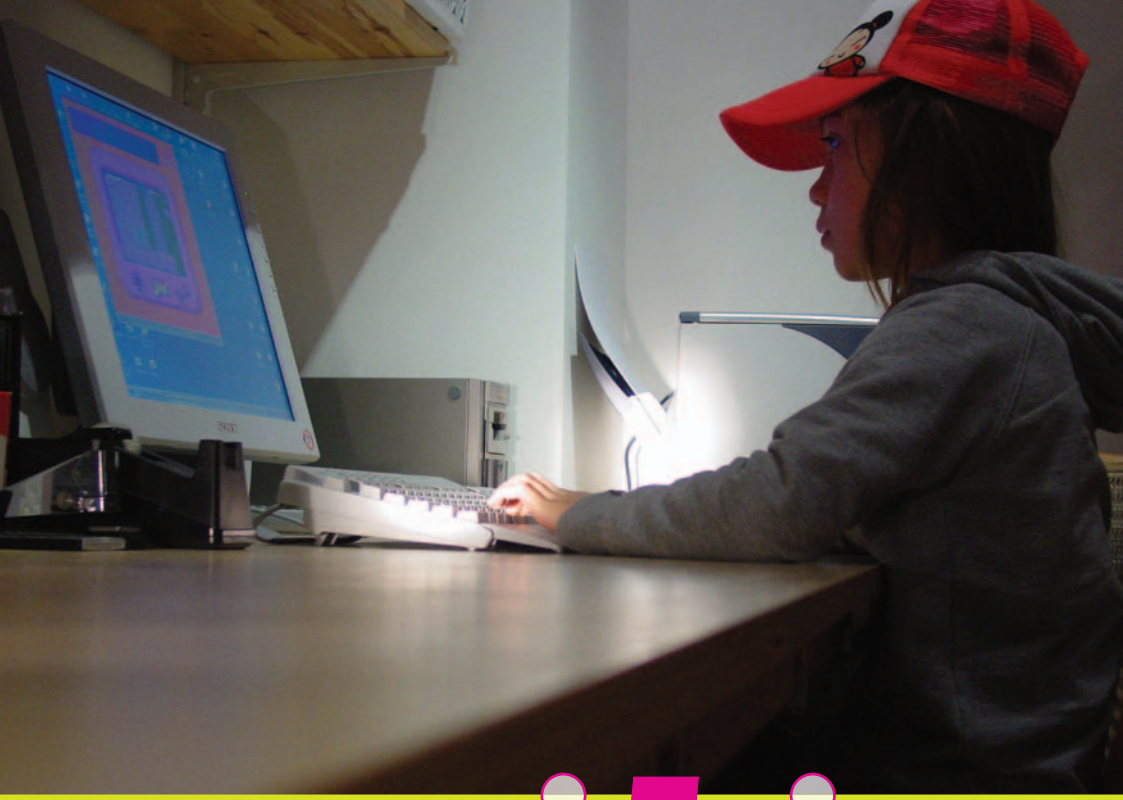


veilig internetten

een beknopte uitleg

surfopsafe.nl

voorwoord

waarschuwen blijft nodig

Voorwoord

Internet is niet meer weg te denken uit ons dagelijkse leven. Thuis, op school of op het werk: bijna iedereen maakt er wel gebruik van. Er zijn steeds meer toepassingen en diensten beschikbaar en mede door het toenemend aantal mensen met een breedbandaansluiting stijgt het internetgebruik snel.

Helaas zijn er op internet ook risico's. Een computer die verbonden is met het internet kan kwetsbaar zijn voor misbruik van buitenaf. Hierdoor kan men zelf schade oplopen, of zonder het zelf te weten schade aan anderen toebrengen. Vooral als thuisgebruiker of kleine zelfstandige bent u niet altijd op de hoogte van alle risico's en hoe u zich daartegen kunt beschermen. In 2001 is de bewustwordings- en voorlichtingscampagne *Surf op Safe* gestart, om juist u als gebruiker informatie te bieden over veilig en betrouwbaar internetgebruik.

Wanneer gebruikers goed op de hoogte zijn van de risico's bij het internetten, herkennen ze gevaren tijdig en weten ze ook hoe ze zich daartegen kunnen beschermen. Deelname aan het internetverkeer is vergelijkbaar met deelname aan het 'gewone' verkeer: je moet de regels kennen, weten wat de borden betekenen en uitkijken bij het oversteken. En tenslotte: een gewaarschuwd mens telt voor twee.

Waarschuwen blijft nodig, ook omdat steeds nieuwe gevaren ontstaan. Daarom ligt nu de tweede editie van de brochure Veilig Internetten voor u.
In deze brochure vindt u een beknopt overzicht van wat u zelf aan uw veiligheid op internet kunt doen. Meer informatie en uitgebreidere tips vindt u op de website www.surfopsafe.nl. Met een aantal eenvoudige maatregelen kunt u op een bewuste en veilige manier gebruik maken van de vele mogelijkheden van internet!

Weet wat u doet! Surf op Safe!

Laurens Jan Brinkhorst
Minister van Economische Zaken

december 2004

algemeen

belangrijke tips

Belangrijke tips

Voordat we ingaan op specifieke aspecten van internetgebruik geven we een aantal tips en richtlijnen die altijd van belang zijn:

- **Gebruik een virusscanner en een firewall.**
- **Houd uw besturingssysteem, virusscanner, browser en andere software veilig,** door regelmatig te kijken of er updates of nieuwe versies beschikbaar zijn. Deze zijn te vinden op de websites van de leveranciers. Gebruik waar mogelijk de automatische updatefunctie.
- **Maak regelmatig een reservekopie** van belangrijke bestanden, brieven, e-mail en digitale foto's en bewaar deze op een veilige plek.
- **Bescherm serieuze zaken met serieuze wachtwoorden.** Gebruik een wachtwoord van minimaal acht tekens, met naast kleine letters een aantal hoofdletters, cijfers en symbolen (!@#$%...).
- **Overweeg lid te worden van een waarschuwingsdienst,** zoals www.waarschuwingsdienst.nl of kijk regelmatig op beveiligings-websites.

surfen

virusscanner en firewall

Surfen

Wanneer u op het internet surft bekijkt u webpagina's met links naar andere pagina's, plaatjes en bestanden. Tijdens het surfen loopt u een aantal risico's. Kwaadwillenden kunnen bijvoorbeeld onveilige bestanden op uw computer installeren. Ook kan men u proberen te verleiden om gegevens af te staan, waarvan vervolgens misbruik kan worden gemaakt.

Door de verregaande automatisering van moderne browsers is het mogelijk dat uw browser zonder uw tussenkomst onveilige bestanden accepteert of gegevens prijsgeeft. Dit kan gebeuren wanneer bij een waarschuwing die de browser geeft ongelezen op 'ja' wordt geklikt, door u zelf, of door andere gebruikers van uw computer. Daarnaast staan de veiligheidsinstellingen van uw browser vaak zo ingesteld dat helemaal geen waarschuwing wordt gegeven. Fouten ('bugs') in uw browser of besturingssysteem kunnen ook gebruikt worden om ongewenste bestanden te installeren of gegevens te vergaren.

Wat zijn de risico's bij het surfen?

- Bedreiging van computer(s) en gegevens, bijvoorbeeld door virussen.
- Misbruik van uw computer doordat deze ongemerkt wordt gebruikt voor het versturen van spam of het uitvoeren van aanvallen op andere computers.
- Aantasting van de persoonlijke levenssfeer en privacy, bijvoorbeeld doordat uw gegevens voor andere doeleinden worden gebruikt dan waar ze voor zijn afgestaan.
- Blootstelling aan ongewenste, bijvoorbeeld erotische, inhoud door confrontatie met webpagina's waar u niet om gevraagd heeft.
- Blootstelling aan malware (zie kader), die tijdens het surfen ongemerkt of door onoplettendheid kan worden geïnstalleerd.
- Verslechtering van de prestaties van uw computer: computers die besmet zijn met een kwaadwillend programma werken vaak trager. Sommige opdrachten worden zelfs helemaal niet meer uitgevoerd.

Hackers, crackers, scriptkiddies

Bij computercriminaliteit wordt vaak gesproken over hackers. Dit is echter niet geheel correct. Beter zijn de termen computercrimineel of cracker. Daarnaast zijn er nog de zogenaamde scriptkiddies: jonge mensen met een relatief beperkte technologische kennis die beveiligingen doorbreken met door anderen gemaakte hulpmiddelen. Ook zij kunnen echter grote schade veroorzaken en ook hun activiteiten zijn crimineel. De correcte betekenis van hacker komt meer in de buurt van 'computerexpert'.

Spyware, adware, browser hijackers, dialers

- **Spyware** maakt zonder toestemming gebruik van uw internetverbinding om illegaal verzamelde informatie naar de verspreider terug te zenden. De term spyware wordt ook gebruikt voor adware (zie hieronder) die het niet zo nauw neemt met de privacy van de gebruiker. Spyware is door slecht programmeerwerk vaak verantwoordelijk voor een instabiel systeem.
- **Adware** is programmatuur die advertenties laat zien en gegevens over surfgedrag terugstuurt in ruil voor het gratis gebruik van een programma of service. In principe is dit volkomen legaal als de gebruiker volledig geïnformeerd is en toestemming heeft gegeven. In de praktijk maakt adware vaak misbruik van het verleende vertrouwen door bijvoorbeeld stiekem informatie terug te sturen naar de verspreider. In deze gevallen wordt adware dus spyware. In de praktijk spreekt men vanwege het moeilijke onderscheid vaak over spyware/adware.
- **Browser hijackers** zijn programma's en scripts die instellingen van uw browser aanpassen, zoals de homepage, de standaard zoekpagina en uw favorieten. Hierdoor verschijnen andere pagina's dan verwacht, vaak verwijzend naar sex- en goksites, en bijna altijd ongeschikt voor kinderen. Ook is het mogelijk dat er extra advertenties in pop-ups verschijnen, zelfs op sites die nooit gebruik maken van pop-ups.
- **Dialers** zijn programma's die ongemerkt het modem dat u gebruikt om te internetten een ander nummer laten bellen dan het 067 nummer van uw provider. Dit kan zelfs als u een breedbandverbinding heeft met daarnaast nog een aangesloten modem. Over het algemeen worden dan 0900 of buitenlandse betaalnummers gebeld tegen hoge tarieven. Overigens zijn er ook legale dialers die u gebruikt om te betalen voor diensten op internet. Net als bij adware/spyware is de lijn tussen deze legale dialers en minder legale dialers erg dun en snel overschreden.

Al deze programmatuur wordt meestal ongemerkt of onder valse voorwendselen op een pc geïnstalleerd.

Malware

Aangezien niet iedereen dezelfde definities voor virussen, trojans, wormen, spyware, adware, browser hijackers en dialers hanteert en wegens het steeds vaker voorkomen van mengvormen wordt al deze 'slechte' software ook wel met de algemene term malware aangeduid, een samentrekking van 'malicious' (Engels voor kwaadaardig) en software.

Wat kunt u doen om de risico's van het surfen te beperken?

- Verhoog de standaard veiligheidsinstellingen en privacy-instellingen van uw browser en e-mailsoftware.
- Gebruik een goede virusscanner en een firewall om uw computer te beschermen. Controleer daarnaast uw computer regelmatig op andere ongewenste bestanden, zoals spyware en adware. Hiervoor zijn goede gratis programma's te downloaden.
- Wees voorzichtig met het verstrekken van persoonlijke gegevens. Ga van tevoren na of de ontvanger van de gegevens betrouwbaar is en of deze de gevraagde gegevens echt nodig heeft. Maak in zo'n situatie eventueel gebruik van een wegwerp (makkelijk vervangbaar) e-mailadres.
- Gebruik een internetfilter als hulpmiddel om kinderen tegen ongewenste inhoud te beschermen.
- Wees, indien er een inbelverbinding op uw computer aanwezig is, alert op dialers die zich ongemerkt op uw computer kunnen installeren en de telefoonkosten kunnen doen oplopen. Verwijder oude inbelverbindingen en niet meer actieve modems.
- Overweeg de installatie van alternatieve software. Veel boosaardige software is specifiek gericht op de meest gangbare programma's.

DDoS en Zombie Netwerk

Wanneer een computer geïnfecteerd is door een worm betekent dit dat de computer een zombie kan worden. Hij kan dan op illegale wijze van buitenaf opdrachten krijgen, bijvoorbeeld om mee te werken aan het versturen van spam of het uitvoeren van een Distributed Denial-of-Service (DDoS) aanval.

Wanneer een grote hoeveelheid computers illegaal 'gecontroleerd' wordt door één persoon of organisatie noemt men deze verzameling computers een zombie netwerk. Bij een DDoS aanval wordt een dergelijk netwerk gebruikt om een website of dienst te bombarderen met aanvragen. De aangevallen computer kan deze stroom van verzoeken niet meer aan en gaat vervolgens uit de lucht. De website, chat of andere dienst is dan onbereikbaar geworden.

e-mailen

reageer nooit op spam

E-mailen

E-mailen biedt de mogelijkheid om wereldwijd tekst te verzenden, maar ook om bestanden zoals plaatjes, video of geluid mee te sturen. E-mail is een goedkope manier om snel te communiceren, indien gewenst ook anoniem. Door deze eigenschappen is e-mail niet alleen een veelzijdig communicatie-middel, maar ook op verschillende manieren te misbruiken.

Wat zijn de risico's bij het e-mailen?

- Door het verstrekken of het gebruik van uw e-mailadres loopt u het risico spam te ontvangen. Dit gebeurt wanneer uw e-mailadres in handen valt van partijen die het niet zo nauw nemen met uw privacy. Dit kan doordat u uw e-mailadres achterlaat op websites, zonder de vaak lange privacy-voorwaarden door te lezen, of doordat een adressenbestand wordt doorverkocht. Maar ook bijvoorbeeld doordat een bekende u een elektronische verjaardagskaart stuurt via een onbetrouwbaar bedrijf.
- Met e-mail worden vaak bestanden meegestuurd als bijlage (attachment). Deze kunnen virussen bevatten, die geactiveerd worden wanneer de bijlage wordt geopend. Dit virus kan er vervolgens toe leiden dat uw eigen computer ongemerkt zelf spam gaat versturen.
- Oplichting via e-mail komt op veel verschillende manieren voor. De bekendste vorm is de zogenaamde Nigeriaanse spam. Potentiële slachtoffers krijgen het verzoek tijdelijk hun bankrekeningnummer beschikbaar te stellen in ruil voor een enorme financiële vergoeding, of om administratiekosten te voldoen in verband met een gewonnen prijs. In de praktijk komt het er op neer dat het contact wordt verbroken en bankrekeningen worden geplunderd.
- Een andere vorm van oplichting is 'phishing', waarbij wordt geprobeerd creditcardgegevens of inloggegevens te verkrijgen door middel van het versturen van een vervalst bericht dat afkomstig lijkt te zijn van een betrouwbare instantie, zoals bijvoorbeeld uw creditcardmaatschappij of bank.
- E-mail wordt onversleuteld verzonden. Partijen die, al dan niet legaal, toegang hebben tot de faciliteiten van de provider van de verzender of geadresseerde kunnen uw e-mail in principe bekijken en lezen zolang u deze niet versleuteld verstuurt.

Virussen

De term virussen wordt meestal breed gebruikt, maar kan verder worden onderverdeeld in ‘echte’ virussen, wormen en trojans.

- **Een virus** is een programma dat zichzelf kan vermenigvuldigen, maar daarvoor een drager nodig heeft zoals een diskette, USB-sleutel, een per e-mail verzonden document, of een gedeeld bestand.
- **Een worm** kan zichzelf verspreiden, bijvoorbeeld door zichzelf door te sturen aan iedereen in uw adresboek of door zelfstandig andere computers op internet op te zoeken.
- **Een trojan (horse)** is een programma dat naast de aangegeven of verwachte functionaliteit nog verborgen eigenschappen heeft die voor misbruik worden aangewend.

Als in deze brochure over virussen wordt gesproken, bedoelen we een virus in de ruimste zin van het woord, dus een virus, trojan of worm.

Hoax

Een **hoax** is een valse viruswaarschuwing waarin de ontvanger wordt aangespoord om maatregelen te nemen, zogenaamd om het virus uit te schakelen. In werkelijkheid is er echter geen sprake van een virus. De maatregelen zijn daarom onnodig en veroorzaken soms zelfs grote schade in de pc. Ook wordt meestal verzocht de waarschuwing aan zoveel mogelijk mensen door te e-mailen, waardoor de hoax als een soort kettingbrief verder wordt verspreid.

Wat kunt u doen om de risico's van het e-mailen te beperken?

- Gebruik een goede virusscanner met de meest recente virusdefinities en wees voorzichtig met het openen van bijlagen. Scan deze alvorens ze te openen.
- Gebruik meerdere e-mailadressen. Verstrek uw belangrijkste e-mailadres alleen aan betrouwbare personen. Gebruik een makkelijk te vervangen (gratis webmail) wegwerpadres als u een partij niet helemaal vertrouwt, maar toch een e-mail-adres moet of wilt afgeven.
- Installeer een spamfilter, of maak gebruik van de faciliteiten die uw provider biedt.
- Reageer nooit op spam. Over het algemeen zijn verzenders van spam niet te vertrouwen. Doordat er toch altijd een klein percentage mensen reageert, blijft spam bestaan. Afmelden of klagen bij de spammer heeft bijna nooit zin. Meld Nederlandse spam bij OPTA via www.spamklacht.nl
- Ga nooit in op e-mails van onbekenden, waarin verzocht wordt om het gebruik van uw bankrekening, briefpapier of andere persoonlijke zaken.
- In principe vragen vertrouwde instanties niet via e-mail om privacygevoelige informatie. Mocht dit toch gebeuren, informeer dan telefonisch bij die instantie of de e-mail echt van hen afkomstig is.
- Versleutel uw e-mail als u zeker wilt weten dat alleen de geadresseerde de inhoud te weten komt.

Spam

De meest gebruikte en geaccepteerde definitie van spam is: ‘Unsolicited Bulk E-mail’ (UBE). In het Nederlands: ongevraagde mail die in grote hoeveelheden wordt verzonden. Vaak bevat spam een commerciële boodschap, maar dit is niet noodzakelijk. In Nederland is het versturen van ongevraagde e-mail aan particulieren onder de meeste omstandigheden verboden.

chatten

voorzichtig met persoonlijke gegevens

Chatten

Chatten is op dit moment een van de meest geliefde activiteiten van jongeren op het internet. Met name het gebruik van MSN Messenger heeft een grote vlucht genomen. Ook datingsites kennen vaak een chatmogelijkheid.

Wat zijn de risico's bij het chatten?

- Door het vermelden van persoonlijke gegevens kan uw privacy of veiligheid gevaar lopen.
- Personen met verkeerde bedoelingen kunnen zich tijdens het chatten als iemand anders voordoen.
- Bij chatten kunnen ook ongewenste berichten worden ontvangen (IM spam, ook wel spim genoemd).
- Kinderen kunnen makkelijk in aanraking komen met voor hen ongeschikte inhoud of personen.
- Pesten via de chatbox komt vaak voor en kan uit de hand lopen.

Wat kunt u doen om de risico's van het chatten te beperken?

- Ga tijdens het chatten altijd zorgvuldig om met het vermelden van persoonlijke gegevens, zoals uw telefoonnummer of uw adres. Kies in eerste instantie altijd een schuilnaam.
- Praat met kinderen over de risico's van chatboxen en MSN en volg hun activiteiten.
- Wees alert op pesten en meld dit aan de chatbox moderator (beheerder).
- Spreek bij ontmoetingen met een onbekende af in een openbare gelegenheid en neem bij voorkeur iemand mee. Zorg in ieder geval dat uw afspraak bij anderen bekend is.

Chatten en IM

Dit is 'babbelen' door het schrijven van vaak korte tekstberichten via internet. Dit kan op openbare of besloten chatboxen of via kanalen op Internet Relay Chat servers (Chatten en IRC). Het kan ook één op één met al dan niet van tevoren bekende contacten (Instant Messaging, IM), zoals bijvoorbeeld met MSN Messenger, ook wel 'MSN-en' genoemd. In deze brochure vatten we alle vormen samen onder het begrip chatten.

delen van bestanden

let op wat je binnenhaalt

Het delen van bestanden

Voor het delen van bestanden met anderen (Peer to Peer of P2P) bestaan speciale programma's. Door bestanden die anderen met u delen opnieuw beschikbaar te stellen verspreiden deze zich over vele computers wereldwijd. Het delen van bestanden wordt vaak gebruikt om muziek en films te downloaden.

Wat zijn de risico's bij het delen en downloaden van bestanden?

- Bij het downloaden van muziek en films gaat het meestal om illegale kopieën, die niet mogen worden verspreid. In Nederland hoeft dit niet strafbaar te zijn indien het om het downloaden van een kopie voor eigen gebruik gaat. Andere landen hebben echter soms een ander beleid.
- Het aanbieden van illegale kopieën is strafbaar. Veel P2P software biedt bestanden die u gedownload heeft automatisch aan andere gebruikers aan. Zelfs indien het downloaden niet strafbaar is, bent u in dit geval wel strafbaar wegens het verder verspreiden.
- Het downloaden van illegaal gekopieerde software is in Nederland strafbaar, ook voor eigen gebruik.
- Gedeelde bestanden kunnen iets anders bevatten dan de naam suggereert. Hierdoor bestaat het gevaar dat u een virus of ander ongewenst bestand binnenhaalt.
- Een aantal veelgebruikte P2P programma's bevat spyware en/of adware.

Wat kunt u doen om de risico's bij het delen en downloaden van bestanden te beperken?

- Gebruik een goede virusscanner om bestanden die u heeft gedownload te scannen.
- Gebruik alleen programma's waarvan bekend is dat ze geen spyware/adware bevatten.
- Bied geen bestanden met illegale inhoud aan.

bestellen en betalen

zorg voor een veilige verbinding

Bestellen en betalen via internet

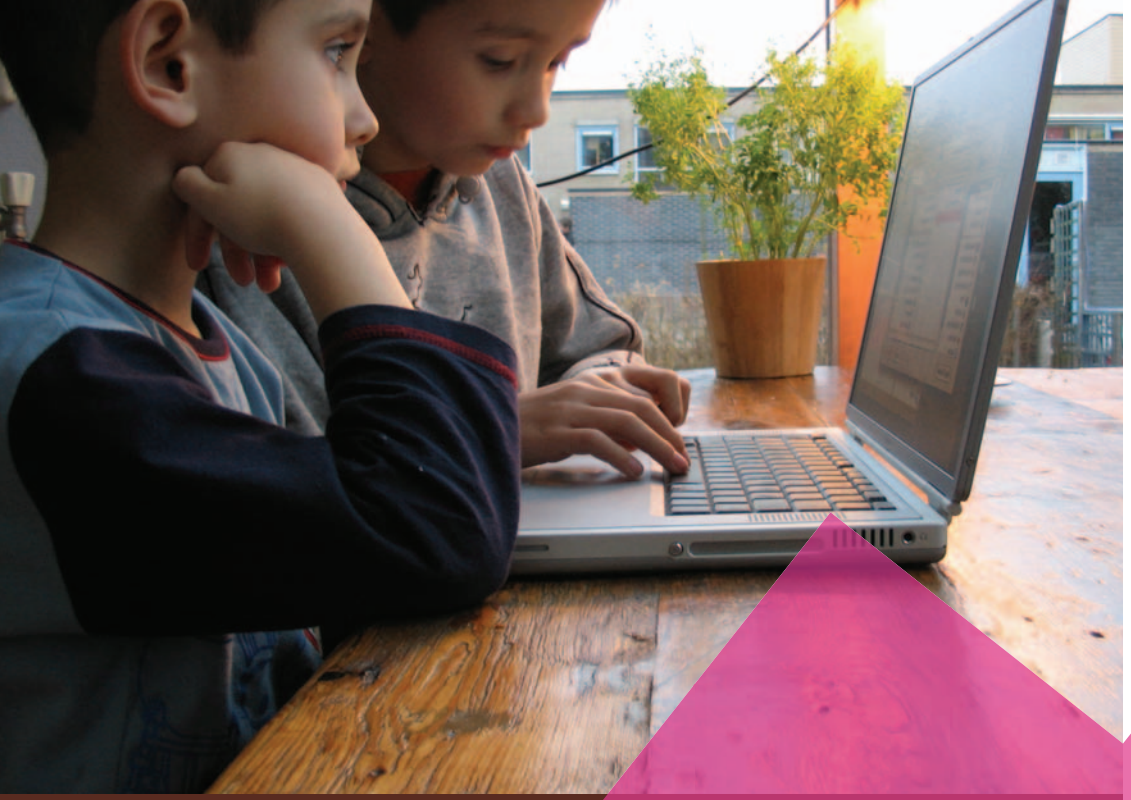
Winkelen op internet neemt in Nederland nog steeds toe. Naast winkels die alleen via internet verkopen, bieden ook steeds meer traditionele winkels hun waren via het web aan. Ook zijn online veilingen en tweedehands verkoop-sites erg populair. Door te winkelen op internet is het mogelijk wereldwijd prijzen te vergelijken en goederen en diensten te bestellen.

Wat zijn de risico's bij bestellen en betalen via internet?

- De bestelde goederen kunnen niet, incompleet, beschadigd, defect of te laat geleverd worden.
- Achteraf kunnen er bijkomende kosten zijn, waardoor de totale prijs hoger uitvalt.
- Misbruik van persoonlijke gegevens, zoals uw e-mailadres.
- Fraude, waarbij u wel betaalt, maar niets ontvangt of waarbij uw creditcardgegevens worden misbruikt.

Wat kunt u doen om de risico's bij het bestellen en betalen te beperken?

- Koop alleen bij internetwinkels waarvan duidelijk is wie erachter zit. Ga na wat de leveringsvoorwaarden zijn, wat het privacy-beleid is en waar u terecht kunt bij klachten of problemen.
- Kijk of de winkel is aangesloten bij een brancheverenigingen, bijvoorbeeld www.thuiswinkel.org.
- Geef uw creditcardgegevens uitsluitend door via een versleutelde verbinding. In uw browser verschijnt onderaan in het scherm een slotje (Internet Explorer) of een sleuteltje (Netscape). Bovendien begint het internetadres van de pagina met 'https' in plaats van 'http'.
- Kijk of er een duidelijke privacy-verklaring is opgenomen op de site en lees deze door.
- Bij sommige internetwinkels kunt u er ook voor kiezen om via acceptgiro en/of onder rembours (bij aflevering door de postbode) te betalen.



draadloos netwerk

gebruik encryptie

Draadloos netwerk

Doordat steeds meer mensen thuis over een makkelijk af te tappen draadloos netwerk beschikken, ligt uw netwerkverkeer als het ware op straat. Misbruik van uw netwerk is te voorkomen door middel van encryptie. Hierbij wordt informatie versleuteld over het draadloze netwerk verzonden.

Wat zijn de risico's van een draadloos netwerk?

- Uw internetverbinding kan door anderen worden misbruikt, terwijl u verantwoordelijk wordt gehouden.
- E-mail en websitebezoek kunnen worden afgetapt.
- Bestanden kunnen worden gekopieerd of gewist.
- Een draadloos netwerk biedt kwaadwillenden de mogelijkheid om ongemerkt uw netwerk af te tappen. De verzamelde gegevens kunnen vervolgens worden gebruikt om op uw netwerk in te breken of om u anderszins te benadelen.

Wat kunt u doen om de risico's van een draadloos netwerk te beperken?

- Gebruik versleuteling. Indien beschikbaar is WPA (Wi-Fi Protected Access) de beste methode. Zo niet gebruik dan de sterkst beschikbare versie van WEP (Wired Equivalent Privacy).
- Als iemand uw netwerk langere tijd gericht kan bestuderen, bijvoorbeeld iemand die in de buurt woont, kan WEP encryptie worden doorbroken. Vervang daarom regelmatig de WEP sleutels.
- Schakel ongebruikte draadloze apparatuur uit.

SSID en MAC-adres filter

Het uitschakelen van de zogenaamde 'SSID broadcast' of het alleen toelaten van netwerkkaarten met een bekend MAC-adres houdt nieuwsgierige buren en voorbijgangers wellicht tegen, maar sneuvelt bij de eerste serieuze inbraakpoging

meer informatie

www.surfopsafe.nl

Meer informatie

Wilt u meer informatie over de in deze brochure genoemde onderwerpen en tips, kijk dan op www.surfopsafe.nl

Hier vindt u ook het laatste nieuws op het gebied van veilig internetten en specifieke informatie en tips over veilig internetten voor bijvoorbeeld kinderen, ouders, docenten en MKB. Ook kunt u uw kennis op het gebied van veilig internet testen en kunt u antwoord krijgen op uw nog resterende vragen.

Wilt u extra exemplaren van deze brochure, dan kunt u deze aanvragen bij de Postbus 51 Informatielijn: telefoon 0800 – 8051 of via www.postbus51.nl

Colofon

Deze brochure is onderdeel van de landelijke voorlichtingscampagne Surf op Safe. Deze campagne is een initiatief van het Ministerie van Economische Zaken en wordt mede ondersteund door de Europese Unie onder het Veiliger Internet programma. Het doel is: zorgen dat internetgebruikers weten welke risico's zij op internet kunnen tegenkomen en dat zij goed in staat zijn zelf maatregelen te nemen om zich te beveiligen. Op die manier kunnen alle Nederlandse internetgebruikers op een verantwoorde, veilige manier gebruik maken van de mogelijkheden van het internet. Surf op Safe richt zich op particulieren en kleine zakelijke gebruikers.

Deze brochure is met grote zorgvuldigheid tot stand gekomen. Aan de inhoud ervan kunnen echter geen rechten worden ontleend.

Projectverantwoordelijkheid: Ministerie van Economische Zaken, Den Haag
Publicatienummer: 04TP38

Basisconcept: Integral, Amsterdam
Fotografie en grafische vormgeving: Kruit *Communicatie en Vormgeving in gebruik,* Montfoort
Druk: Drukkerij Hendrix, Peer

Ministerie van Economische Zaken

Information Society Technologies

veilig internetten, een beknopte uitleg

surfopsafe.nl