5. Veilig e-mailen en bestellen op internet

Mogelijk ontvangt u regelmatig ongewenste e-mail. Voorbeelden daarvan zijn phishingmails, spam, hoaxes en kettingbrieven. Veel van deze e-mails worden tegenwoordig al tegengehouden door uw e-mailaanbieder, maar ook u kunt enkele acties ondernemen om ongewenste e-mail te voorkomen en verwijderen. In dit hoofdstuk leest u hierover.

Op internet is zeer veel te koop. Boeken, wasmachines, fietsen, auto's, sieraden, computers, kleding, teveel om op te noemen. Ook kunt u een dagje uit of vakantie online boeken en betalen.

Via een webwinkel kunt u producten of diensten tegen betaling bestellen. Als koper kunt u zo op internet vanuit uw stoel achter de pc inkopen doen. Uw bestelling wordt in veel gevallen thuisbezorgd.

Voor de betaling van deze producten en diensten zijn diverse mogelijkheden. De verkoper bepaalt welke betalingsopties hij aanbiedt. U als koper moet daarmee akkoord gaan als u het product wilt aanschaffen. Daarbij moet u letten op de veiligheidsaspecten van de betalingen en de leverings- en garantievoorwaarden.

U krijgt in dit hoofdstuk informatie over allerlei aspecten van online aankopen doen, zoals de betaalmethode en het herkennen van een veilige website. Het is bedoeld om door te lezen zodat u gerichte keuzes kunt maken als u overgaat tot kopen via internet. Ten slotte leest u hoe u producten kunt bestellen via de webwinkel van Bol.com.

In dit hoofdstuk krijgt u informatie over:

- phishing, spam, hoaxes en kettingbrieven;
- veilig e-mailgedrag;
- betaalmethoden op internet;
- een veilige website herkennen;
- Thuiswinkel Waarborg;
- bestellen op een website.

5.1 Phishing

Het internet wordt door steeds meer mensen gebruikt voor online bankieren, winkelen, vliegtickets bestellen, verkoop van tweedehands spullen, studeren, enzovoorts. Helaas hebben criminelen inmiddels ook hun weg op internet gevonden. Eén van de criminele activiteiten die steeds vaker wordt beoefend, staat bekend als *phishing*. Maar wat is phishing nu precies?

Phishing is een methode om argeloze computergebruikers over te halen hun persoonlijke gegevens of financiële informatie op te geven. Phishing is in feite 'vissen' naar informatie.

Een veelgebruikte phishing truc begint met een nep e-mailbericht dat eruit ziet als een officieel bericht van een bekende, betrouwbare bron. Dat kan uw bank, uw creditcardmaatschappij, een internetwinkel of een andere website zijn die u al eens bezocht heeft. Zo'n bericht wordt verzonden naar tienduizenden e-mailadressen.

In het e-mailbericht wordt aan de ontvangers gevraagd om bijvoorbeeld hun bankgegevens te controleren. In de e-mail staat daarvoor een hyperlink die leidt naar een website die exact lijkt op de website van een bankinstelling. Daar wordt gevraagd om ter controle persoonlijke informatie in te vullen, zoals naam en adresgegevens, bankrekeningnummers en pincodes.

Als u erin trapt en uw gegevens invult, wordt de informatie direct verzonden naar de criminelen die deze valstrik hebben opgezet. Vervolgens gebruiken ze uw gegevens om spullen te kopen, nieuwe creditcardrekeningen te openen op uw naam of op een andere manier misbruik te maken van uw identiteit. Deze phishing e-mails en websites lijken bedrieglijk echt. Vaak wordt het logo van een bankinstelling gebruikt in de e-mail. De websites worden exact nagemaakt.

Een voorbeeld van een phishingmail:

Deze roept ING-klanten op hun persoonsgegevens in te vullen via een website, waarna de criminelen de bankrekening kunnen plunderen.

ING

Leeuwarden, 31 mei ID: 782H.92001

Betreft: onderhoud Mijn ING

Geachte Mijn ING Klant,

Vanwege een toename aan fraude op Mijn ING zijn wij genoodzaakt een systeemupdate uit te voeren.
Dit houdt in dat u eenmalig uw I.P. adres aan uw Mijn ING rekening moet verbinden. Door uw verificatie kunnen wij ongeautoriseerde betalingen voorkomen.

Voor het juist uitvoeren van deze verplichte systeemupdate, dient u op de onderstaande beveiligde hyperlink te klikken.
Deze verwijst u naar de beveiligde Mijn ING inlog/update scherm. De onderstaande hyperlink is eenmalig geldig en is verbonden met uw actuele Mijn ING gegevens.

Volg de volgende hyperlink: https://mijn.ing.nl/internetbankieren/SesamLoginServlet

Wij danken u voor uw medewerking.

Met vriendelijke groet,
ING Nederland

Team Online Fraude & Security

Let op!

Criminelen beperken zich niet meer tot alleen online phishing. Er worden steeds meer gevallen bekend waarbij het slachtoffer thuis wordt opgebeld door een zogenaamde medewerker van hun bank, van het niet bestaande '*Windows Maintenance Team' ('Windows Onderhoudsteam')* van Microsoft, of van een andere officieel klinkende instantie.

Deze persoon vraagt (vaak in gebrekkig Nederlands of Engels) om bepaalde zaken op de computer te regelen. Meestal met de smoes dat de beveiliging van de computer niet in orde is. De ene keer moet het slachtoffer zelf instellingen aanpassen, de andere keer doet de zogenaamde medewerker van de bank het zelf via een programma waarmee hij op afstand toegang tot uw computer krijgt terwijl het slachtoffer meekijkt. Vaak wordt tussen neus en lippen door om persoonlijke codes en wachtwoorden voor internetbankieren gevraagd.

Ga hier niet op in! Medewerkers van *Windows* of Microsoft zullen u nooit thuis bellen over problemen met uw computer. Ook uw bank zal u nooit bellen om instellingen van uw computer te veranderen, of om u te vragen naar uw persoonlijke codes voor internetbankieren.

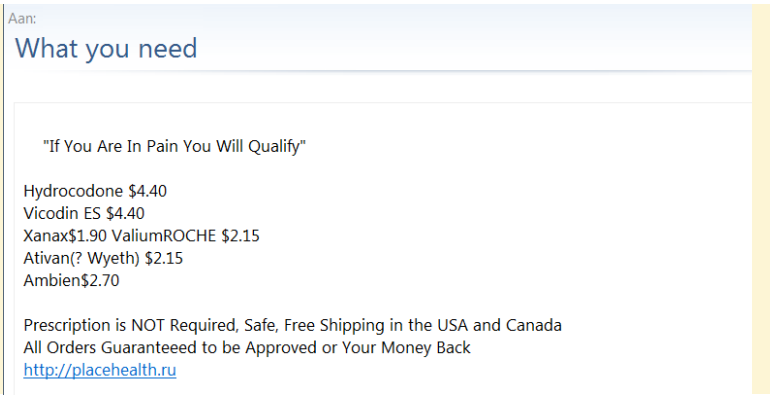
5.2 Spam

Spam zijn e-mails met commerciële reclame die ongevraagd aan u worden gestuurd. Dagelijks gaan er honderden miljoenen van deze e-mails internet over. Ze worden gebruikt om allerlei producten te verkopen, meestal medicijnen zoals Viagra en pijnstillers, maar ook horloges en sieraden.

De bedoeling van spam is u naar een bepaalde website te lokken en producten te laten kopen. De verkopers achter de producten zijn vaak oplichters die waardeloze of illegale producten leveren of gewoon niets leveren terwijl u betaald heeft.

Soms zijn dit ook legale bedrijven uit het buitenland, maar aangezien spam versturen in steeds meer landen verboden is, is de kans klein dat een betrouwbaar bedrijf zich hier nog mee bezig zou houden. U moet dus nooit op dit soort reclamemails ingaan.

Een voorbeeld van spam:



Aangezien er toch nog altijd een klein percentage van de computergebruikers ingaat op spam, blijft het een lucratieve bezigheid voor spammers om spammails te versturen. Het sturen van een e-mail kost hen zeer weinig tot niets. Vaak maken ze gebruik van een netwerk van gehackte computers. Deze computers zijn eerder op illegale wijze overgenomen en kunnen nu door deze lieden van afstand worden gebruikt. E-mailadressen hebben ze ook vaak op deze manier binnengehaald.

Het vervelende van spam is dat uw mailbox vol komt te zitten met nutteloze e-mails, die u iedere keer moet weggooien. Zonder voorzorgsmaatregelen kunt u zo honderd spammails per dag krijgen.

Internetaanbieders hebben tegenwoordig spamfilters waarmee ze de meeste spam al op hun eigen servers tegenhouden voordat de e-mail uw e-mailaccount bereikt.

Daardoor zult u al veel minder spam op uw computer ontvangen. Toch is het verstandig ook op uw eigen computer maatregelen tegen spam te nemen. Sommige antivirusprogramma's bieden ook bescherming tegen spam.

Let op!

Niet alle reclamemail is spam. Als u zich eerder vrijwillig heeft aangemeld bij een bedrijf met uw e-mailadres, is er een mogelijkheid dat u van dat bedrijf reclame via e-mail zult ontvangen. Meestal kunt u dit overigens al opgeven bij het aanmelden op de website. Wilt u geen reclame e-mail meer van dit bedijf ontvangen, dan kunt u dit bij het bedrijf melden.

Houd er wel rekening mee dat ook sommige spammers in hun e-mails aanbieden om de reclame te beëindigen. U moet daarvoor op een hyperlink in de e-mail klikken. U wordt dan echter niet uitgeschreven, maar u stuurt juist een bevestiging dat uw e-mailadres correct is, zodat men er nog meer spam naartoe kan sturen. Doe dit dus alleen bij betrouwbare, bekende bedrijven waarvan u weet dat u daar eerder een bestelling heeft gedaan of uw e-mailadres heeft opgegeven.

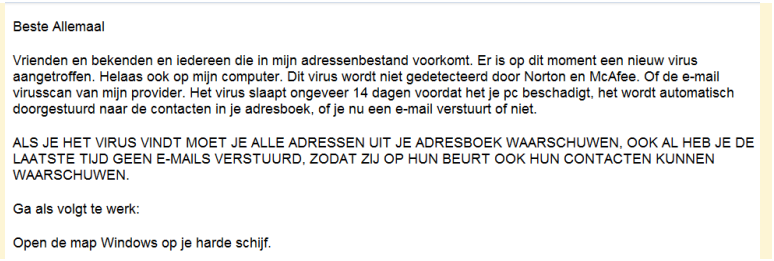
U kunt een klacht indienen over spam via www.spamklacht.nl

5.3 Hoaxes en kettingbrieven

Hoaxes en *kettingbrieven* zijn e-mailberichten die met één reden zijn geschreven: u aanzetten om deze door te sturen naar iedereen die u kent. De inhoud van deze berichten is doorgaans niet waar.

Hoaxes zijn bijvoorbeeld e-mails die een valse viruswaarschuwing geven. Vaak wordt in zo'n mail precies beschreven hoe u een bepaald virusbestand op uw harde schijf moet opzoeken en verwijderen. Vaak is dat een *Windows*-systeembestand. Als u die aanwijzingen zou opvolgen, werkt *Windows* niet goed meer. In feite bent u dan zelf het werkelijke virus. U beschadigt immers zelf uw computer. Volg nooit de instructies en stuur ze niet door naar anderen.

Een voorbeeld van een hoax-mail met als onderwerp *LET OP! GEVAARLIJK NIEUW VIRUS ONTDEKT!*:



Beste Allemaal

Vrienden en bekenden en iedereen die in mijn adressenbestand voorkomt. Er is op dit moment een nieuw virus aangetroffen. Helaas ook op mijn computer. Dit virus wordt niet gedetecteerd door Norton en McAfee. Of de e-mail virusscan van mijn provider. Het virus slaapt ongeveer 14 dagen voordat het je pc beschadigt, het wordt automatisch doorgestuurd naar de contacten in je adresboek, of je nu een e-mail verstuurt of niet.

ALS JE HET VIRUS VINDT MOET JE ALLE ADRESSEN UIT JE ADRESBOEK WAARSCHUWEN, OOK AL HEB JE DE LAATSTE TIJD GEEN E-MAILS VERSTUURD, ZODAT ZIJ OP HUN BEURT OOK HUN CONTACTEN KUNNEN WAARSCHUWEN.

Ga als volgt te werk:

Open de map Windows op je harde schijf.

Andere hoaxes bevatten verhalen over iemand die ziek is of hulp nodig heeft. Door deze berichten te versturen naar andere mensen wordt zogenaamd geprobeerd geld in te zamelen. Deze berichten zijn vrijwel altijd onbetrouwbaar en alleen bedoeld om u geld uit de zak te kloppen.

Kettingbrieven hebben dezelfde opzet als hoaxes. Deze berichten bieden meestal geld of geluk als u de berichten doorstuurt. En natuurlijk ongeluk als u dat niet doet. Kettingbrieven worden vaak gebruikt om e-mailadressen te verzamelen en ze te verkopen aan commerciële organisaties.

U ontvangt een hoax of kettingbrief meestal van een vriend of bekende. Hierdoor gelooft u het verhaal misschien sneller. U moet altijd zelf eerst onderzoeken of de informatie in de e-mail juist is. Een goede bron van informatie is www.virusalert.nl. Laat de persoon die een hoax naar u heeft gestuurd altijd weten dat het een waarschuwing voor een nepvirus is en wijs hem of haar op deze website.

5.4 Veilig e-mailgedrag

U kunt als volgt uw computer nog veiliger houden door middel van uw e-mailgedrag:

- Open nooit berichten van onbekende verzenders. Verwijder ze onmiddellijk.
- Worden er in het bericht spectaculaire aanbiedingen, prijzen of wondermiddelen aangeboden? Beantwoord deze mails nooit en klik nooit op een eventueel aanwezige hyperlink. Door dat te doen, laat u de verzender weten dat uw e-mailadres in gebruik is. Dit veroorzaakt alleen maar meer spam.
- Niet ieder phishingbericht wordt als zodanig herkend. Beantwoord nooit berichten van banken, creditcardbedrijven of internetwinkels waarin persoonlijke informatie wordt gevraagd. Deze e-mailberichten lijken vaak bedrieglijk echt, maar zijn altijd nagemaakt.
- Wees voorzichtig met uw e-mailadres. Geef het niet aan iedereen door. Vul het niet zomaar in op iedere website. Voordat u het weet ontvangt u allerlei spam en ongewenste berichten. Er is een levendige handel in e-mailadressen.
- Overweeg een extra e-mailadres te nemen. Het eerste adres is voor vrienden, familie en werk. Het tweede is om in te vullen op websites. Als u teveel berichten ontvangt op het tweede adres, kunt u nog een derde adres nemen.
- Bedenk dat verwijderde berichten in de map *Ongewenste berichten* worden opgeslagen en dat u deze map ook moet legen.
- Zorg er altijd voor dat u een goed up-to-date antivirusprogramma heeft.