

## Internetvalkuilen op je werk

**Internetgebruik op het werk is een voortdurende bron van discussie. Wat mag een werknemer wel en wat mag hij of zij niet. En, net zo belangrijk, wat mag de werkgever wel en niet. Daarnaast liggen er gevaren bij het surfen op het internet op de loer in de vorm van virussen, hackers en spyware. Als secretaresse zul je ongetwijfeld veel met het internet werken. Daarom is het belangrijk om te weten waar je op moet letten in de jungle die het internet soms is. Dit artikel laat zien hoe je je door deze jungle moet bewegen.**

door: Gabor Mooij

### Voorbeeld

Stel je voor dat een collega voor privé-zaken gebruik heeft gemaakt van je PC. Hij heeft uitgebreid zitten kijken op de website van een webwinkel. Jij hebt pauze en als je terugkomt, zie je de webwinkel op je scherm staan. Dan vraagt je baas of je even bij hem komt. "Ik liep net langs je PC en zag de site van een winkelsite op je scherm staan. De netwerkbeheerder zei dat er vanaf die PC een half uur privé is gesurfd op het internet. Daar ben ik niet blij mee." Je moet dan uitleggen dat je weg bent geweest en dat iemand anders je PC heeft gebruikt. De baas gelooft je, maar drukt je op je hart voortaan beter op je PC te letten. Je gaat met een rot gevoel weer aan het werk en probeert erachter te komen wie er op je PC heeft gezeten. Helaas heeft niemand iets gezien omdat de deur van je werkkamer dicht was. Je wilt het een volgende keer voorkomen. "Voortaan log ik maar uit voordat ik naar buiten ga", besluit je voor jezelf.

Een paar weken later kom je terug van de pauze en op je scherm staat een pornosite. Voor je toetsenbord zie je het briefje liggen waarop je je wachtwoord en gebruikersnaam voor het internet hebt staan. Normaal zit dat aan de rand van je scherm gekleefd. De systeembeheerder komt bij je langs en vraagt je waarom er pornosites vanaf je PC worden bezocht." Je geeft aan dat er misbruik van de PC is gemaakt en dat jij absoluut geen pornosites bezoekt. De systeembeheerder neemt dat van je aan, maar waarschuwt je dat als het nog een keer gebeurt het bedrijf je moet ontslaan. Je schrikt je rot. "Kan ik zomaar ontslagen worden vanwege het bezoek aan een website?", vraag je je bij jezelf af.

Nog steeds is niet duidelijk wie je PC heeft gebruikt. Dit geeft je een rot gevoel, blijkbaar kun je niet al je collega's vertrouwen. Je haalt het briefje met je wachtwoord weg bij de PC en gaat naar de systeembeheerder om te vragen of die je wachtwoord wil veranderen. Ook vraag je hem of hij kan uitzoeken wie steeds stiekem achter je PC gaat zitten. Helaas kan hij dat niet direct aangeven, omdat er steeds gebruik is gemaakt van jouw inloggegevens.

Dan blijkt dat je PC is besmet met een virus. Degene die op je PC internette, heeft ook gemailed en er kwam een mailtje met een bijlage binnen dat jij hebt geopend. Daardoor verspreidde zich in hoog tempo een virus op je PC. Al je documenten zijn door het virus getroffen en een deel ervan kan niet meer worden hersteld. De stiekeme internetter maakte op je PC gebruik van een anonieme emailadres zodat nog niet direct duidelijk is om wie het gaat. Je wordt niet ontslagen, omdat aangetoond kan worden dat het met het eerdere internetbezoek te maken had, maar voor jou is al je werkplezier verdwenen.

Uiteindelijk wordt de internetmisbruiker wel betrapt. De netwerkbeheerder komt er via speciale detectiesoftware, waarmee emailverkeer wordt gevolgd, achter wie jouw PC en die van een aantal anderen misbruikte. Deze persoon wordt vervolgens op staande voet ontslagen. Jij hebt je lesje geleerd en zorgt wel dat er niemand meer op je PC kan en aan je inloggegevens kan komen als jij niet in de buurt bent. Ook let je voortaan op de mailtjes die je krijgt. Als het geen mailtje is van een afzender die je kent, maak je de bijlagen niet meer open. Op die manier voorkom je dat je nog een keer avonden moet overwerken om oude documenten opnieuw in te typen.

### Misbruik

Het bovenstaande voorbeeld laat zien hoe internetgebruik je op je werk in de problemen brengen. In Nederland zijn inmiddels honderden mensen ontslagen vanwege internetmisbruik. Een kwart van de Britse bedrijven heeft om die reden al eens een medewerker ontslagen.

Wat wordt in Nederland nou precies wel en niet als internetmisbruik gezien? De Nederlandse rechter staat ontslag vaak niet toe als een bedrijf niet duidelijk heeft gemaakt aan een werknemer wat wel en

niet mag bij het internetverkeer. Met één uitzondering: rechters zien het versturen van erotische mailtjes en het bezoeken van pornosites bijna altijd als voldoende reden om een arbeidscontract te beëindigen. Het is belangrijk dat jij weet welke afspraken er in je bedrijf gelden op het gebied van internetgebruik en emailverkeer. Als hier geen regels voor zijn dan is het aan te raden om dit onderwerp op je werk ter sprake te brengen.

Overigens is het een misverstand dat internetmisbruik op het werk vooral het bezoeken van sekssites en het rondsturen van erotische mailtjes is. Het kan net zo goed gaan om het boeken van een reis op een vakantiesite of bijvoorbeeld het bezoeken van nieuwsgroepen over tweedehands wagens. Als de werkgever dit duidelijk verbiedt, is er een grond voor ontslag.

Er is een grens aan wat een bedrijf wel en niet mag verbieden. De Wet bescherming persoonsgegevens geeft aan dat de werkgever de privacy van de werknemer moet respecteren. Zo mag een werkgever niet zomaar het computergebruik van de werknemer controleren en verbieden. Hiervoor moet sprake zijn van een gerechtvaardigd belang. Dat kunnen kosten zijn. Als iemand teveel internet, is hij of zij niet productief meer. Het kan ook veiligheid zijn. Het bezoeken van sites en het mailen kan risico's met zich meebrengen voor het bedrijfsnetwerk en het vergroot de risico dat bedrijfsgeheimen uitlekken. Verder mag de werkgever internetverkeer controleren als werknemers in hun functioneren worden belemmerd door bijvoorbeeld seksuele intimidatie. Van een gerechtvaardigd belang is geen sprake van als jij af en toe mailt met vrienden of familie of als je in beperkte mate sites bezoekt voor privégebruik.

Het College Bescherming Persoonsgegevens (CBP) heeft een gedragscode voor internetgebruik opgesteld. Deze regels houden in dat enig privégebruik van email en Internet op het werk mogelijk moet zijn.

Een ander probleem is de aansprakelijkheid. Stel dat jij illegale mp3'tjes kopieert van het internet en de werkgever vervolgens een schadeclaim krijgt wegens het downloaden van die bestanden. Dan kan dat voor de werkgever een reden zijn om je te ontslaan. Een oplossing hiervoor is volgens WebLimits, een bedrijf dat zich bezighoudt met verantwoord internetgebruik, dat werkgever en werknemers een lijst maken waarop staat welke sites wel en niet mogen worden bezocht.

Voor de controle op internetten en email kunnen werkgevers gebruik maken van speciale software. Het gaat om programma's waarmee bijvoorbeeld emails, bezochte websites en toetsaanslagen worden geregistreerd. Er is zelfs software die regelmatig vastlegt wat er bij iemand op het beeldscherm staat. Deze controles mogen echter de belangen van de werknemer niet schaden als het gaat om diens privacy, diens vrijheid van meningsuiting en diens recht op bepaalde informatie. Het is echter moeilijk te bepalen of een werkgever zich hier aan houdt, omdat de programma's alles vastleggen wat je doet.

## **Bedreigingen**

In het voorbeeld aan het begin van dit artikel was sprake van een besmetting van de PC met een virus door het openen van de bijlage bij een mailtje.

Virussen kunnen via mailtjes of via het internet op je PC komen. Een virusbesmetting kan trouwens ook optreden na het kopiëren van bestanden van bijvoorbeeld een cd. Virussen kunnen worden tegengehouden met een zogeheten virusscanner. Software die voortdurend bijgewerkt moet worden om besmetting door de nieuwste virussen te voorkomen. Als het goed is, gebeurt dit door de systeembeheerder. Als je dit niet zeker weet, is het verstandig om hier navraag naar te doen. Naast de besmetting door een virus zijn er nog vele andere risico's die het surfen met zich meebrengt. Allereerst is er de zogeheten spyware. Dit zijn bestanden die zonder dat jij dat door hebt, vanaf je PC boodschappen verzenden naar een externe computer. Naar schatting is zeventig procent van alle computers met spyware besmet. Bij spyware kan het om een programmaatje gaan dat aan een marketingbedrijf doorgeeft welke sites je bezoekt. Dit soort spyware zit vaak verstopt in muziekdownloadprogramma's, zoals Kazaa. Daarnaast is er spyware die gevoelige bedrijfsinformatie naar buitenstaanders verzendt. Denk bijvoorbeeld aan een bankmedewerker die bestanden downloadt en daarbij spyware binnenhaalt die vervolgens klantgegevens zoals pincodes of creditcardgegevens verstuurt aan criminelen.

Hoe voorkom je spyware? Het effectiefst is het niet downloaden van bestanden die niet met je werk te maken hebben. Spyware is namelijk moeilijk te detecteren en lastig van je PC te verwijderen. Er bestaat software om spyware te verwijderen. Dit verwijderen kost echter veel tijd.

Een geheel andere bedreiging wordt gevormd door 'phishing'. Dit is een vorm van oplichting waarbij een website letterlijk wordt gekopieerd. Het adres van de site ziet er door het gebruik van niet-ASCII-tekens net uit als dat van de originele site. Ook kan bijvoorbeeld een l vervangen zijn door een hoofdletter l. In [www.google.nl](http://www.google.nl) merk je niet direct dat de l vervangen is door een hoofdletter l. Je krijgt een mailtje dat afkomstig lijkt van een site waar je misschien bankiert of winkelt. Als je dan een link in

dit mailtje aanklikt en vervolgens op de namaaksite gegevens invoert zoals wachtwoorden, creditcardnummers en pincodes, worden die gegevens rechtstreeks naar de oplichters gestuurd. Deze gebruiken de gegevens vervolgens op de echte site. Het beste is om nooit gebruik te maken van dit soort links en altijd zelf het webadres in te tikken. Een andere optie is te controleren uit welke tekens de link precies bestaat.

Met phishing houdt de trukendoos van de internetoplichters nog niet op. Er kan ook nog sprake zijn van scam. Dit zijn mailtjes waarin je bijvoorbeeld wordt meegedeeld dat geheel onverwacht een prijs is gevallen op je emailadres. Als je dan gaat reageren wordt er eerst gevraagd om een bepaald bedrag te storten bij een advocatenkantoor om daarmee de uitkering van het geld mogelijk te maken.

Vervolgens hoor je niets meer. Een andere vorm van scam is de zogeheten Nigerian-connection. Hierbij vraagt een vermogend persoon, bijvoorbeeld een politicus die is afgezet, om financiële steun met de belofte dat je later ruim voor je bijdrage beloond zal worden. Je betaalt en je raadt het misschien al, je hoort nooit meer iets van de politicus, die zelf van de hele zaak waarschijnlijk niets afweet.

### **Veilig**

Aan het gebruik van het internet op het werk kleven dus vele risico's. Zowel wat de relatie met je werkgever betreft als met betrekking tot het veilig werken met je computer. Gelukkig telt een gewaarschuwd mens voor twee. Zolang je je bewust bent van de gevaren en hier rekening mee houdt, trap je niet snel in één van de internetvalkuilen. De volgende tips helpen je om met een gerust hart gebruik te maken van internet en email op je werk:

- Log uit op je PC als je je werkplek langere tijd verlaat.
- Zorg dat anderen nooit je inloggegevens kunnen zien.
- Bekijk wat voor regels je werkgever heeft voor internetgebruik; vraag je werkgever ernaar als deze er niet zijn.
- Stel met je werkgever en collega's een lijst op met websites die je wel en niet mag bezoeken.
- Maak maar beperkt gebruik van email en het internet voor privégebruik.
- Ga nooit illegale bestanden downloaden op je werk.
- Open geen bijlage(n) bij een mailtje van een onbekende afzender.
- Check of er een virusscanner op je PC zit en of de virusbescherming actueel is.
- Zet geen bestanden op je PC die spyware kunnen bevatten, zoals muziekprogramma's en spelletjes.
- Klik nooit zomaar op een link die in een mailtje staat. Zeker niet als je op de website iets wilt kopen of geld wil overmaken. Kijk altijd eerst of de link wel naar de goede site verwijst.
- Trap niet in mailtjes waarin je een prijs wordt beloofd of waarin om financiële steun wordt gevraagd.