E-mail-etiquette

E-mail is niet meer weg te denken uit onze dagelijkse communicatie, zowel privé als op het werk. Vroeger ging alles via telefoon of via brief en e-mail heeft het ons erg gemakkelijk gemaakt. Maar aan alle goede kanten is vaak ook een keerzijde verbonden. De snelheid waarmee e-mails opgemaakt en verzonden kunnen worden en de gemakkelijkheid waarmee ze beantwoord en doorgestuurd kunnen worden houdt het risico in dat er doelbewust of onvrijwillig misbruiken kunnen gebeuren. Daarom willen we in deze bijdrage enkele mogelijke risico's onder ogen brengen en tips geven voor een correcter e-mailverkeer voor je organisatie, voorziening of school.

Mag men ontvangen e-mails zomaar doorsturen ?

Collega Jan stuurt een verontwaardigde mail naar collega Piet waarin hij zich beklaagt over diens manier waarop hij in een vergadering door Piet aangepakt werd. Collega Piet pikt deze opmerking niet en stuurt de integrale e-mail prompt door naar zijn baas, die enkele dagen later Jan op het matje roept omwille van een ongepaste e-mail. Jan is verbijsterd. Hij had deze e-mail niet naar zijn baas gestuurd en is verrast maar ook wel boos dat zijn baas dit te lezen kreeg. Dit was niet het opzet van zijn reactie aan collega Piet. Hij wilde naar hem reageren en vindt dat die mail niet doorgestuurd had mogen worden en beschouwt het als een vorm van klikken. Nog erger vindt hij dat hij nu bij zijn baas op het matje geroepen wordt, terwijl dat nooit de bedoeling van zijn e-mail was.
Gelijkaardig. Mieke zit als vrijwilligster in een organisatie en beklaagt er zich bij Anja via mail over dat vrijwilligster Katrien verkeerde beslissingen genomen heeft. Anja stuurt de mail zonder medeweten van Mieke door naar Katrien, die verbijsterd is over deze reactie en meteen antwoordt rechtstreeks aan Mieke, maar met in CC de hoofdverantwoordelijke van de organisatie. Enkele dagen later moet Mieke het gaan uitleggen bij de hoofdverantwoordelijke én bij Katrien, hoewel de e-mail voor geen van beiden bedoeld was.

In deze beide situaties werden met enkele snelle eenvoudige klikjes op het toetsenbord heel ernstige drama's veroorzaakt. Enige tijd geleden werd in een organisatie een medewerker ontslagen omdat hij zich via mail bij een collega had beklaagd over de gebrekkige organisatie en de slechte leiding. Deze collega , die het wel eens was met deze bemerkingen, stuurde de mail door naar een collega met enkele aanvullingen, die het op zijn beurt naar een groep collega's doorstuurde samen met enkele bedenkingen. Dit gebeurde zo enkele keren, tot iemand in rang 4 of 5 van ontvangers van deze e-mail, onnadenkend een reactie verstuurde naar de hele personeelsgroep onder een groepsnaam van de hele organisatie, waarin ook de directie zat, zodat de mail ook bij de directie belandde. Helemaal onderaan de lange mail met diversie bedenkingen, reacties en aanvullingen stond de oorspronkelijke mail van de collega die het eerst een bericht stuurde naar een bevriende collega. De directie vond de die reactie van het allereerste bericht onbetamelijk en aanstootgevend en ondermijnend voor de hele organisatie en ontsloeg de medewerker op staande voet. Voor de arbeidsrechtbank werd uiteindelijk dit ontslag omgezet in een ontslag met opzegvergoeding en schadevergoeding omdat bleek dat deze mail in eerste instantie niet aan de directie werd verstuurd en de privacy met voeten werd getreden, maar het ontslag zelf werd niet ongedaan gemaakt. Hoe enkele klikjes op het toetsenbord zeer zware gevolgen hadden….

Met deze voorbeelden wil ik aantonen dat het gevaarlijk is om e-mails die men krijgt onnadenkend door te sturen naar collega's of andere personen. Vooreerst is het strafbaar wegens schending van de privacy-wetgeving omdat betrokkene geen toestemming heeft gegeven om het bericht door te sturen, maar anderzijds schuilt ook het risico dat in de hele weg van doorsturen, iemand het oorspronkelijke bericht kan aanpassen en zo schade kan berokkenen aan de oorspronkelijke schrijver, zeker als deze laatste het veranderde bericht niet meer onder ogen krijgt, maar heel wat andere personen dit aangepaste bericht kunnen lezen, denkend dat het origineel van betrokkene kwam.

Op de website van de faculteit Rechten van KULeuven krijg je wat meer uitleg over doorsturen van e-mails en relatie met privacy. http://cwisdb.kuleuven.be/pisa/nl/juridisch/privacy.htm

Een van de vragen is . Mag men ontvangen e-mail doorsturen naar iemand anders? Mag persoon A, die e-mail krijgt van persoon B, deze mail doorsturen naar persoon C zonder medeweten van persoon

B? Mag men e-mails die men van iemand ontvangt zonder zijn toestemming publiek (= posten in netnews, publiceren op het web, ...) maken?

De bescherming van artikels 259bis en 314bis§2 zouden hier enige verklaring kunnen bieden. Deze artikels beschermen het inkijken van andermans communicatie. Het onderscheid tussen de twee bepalingen uit het Strafwetboek ligt in de hoedanigheid van de dader: artikel 259bis geldt voor ambtenaren, art. 314bis voor andere personen (burgers). Beide artikels beschermen het telecommunicatiegeheim en verbieden principieel om andermans privé-communicatie af te luisteren. Deze artikels beschermen de inhoud van telecommunicatie, dit is de eigenlijke substantie van de telecommunicatie, zoals een gesprek over de telefoon of de tekst van een e-mail bericht. Niet alleen het inkijken is strafbaar, ook het opnemen ('saven') ervan. Indien men later deze opname gebruikt of aan anderen doorgeeft, worden er eveneens straffen voorzien. Het is bovendien niet vereist dat de beklaagde zelf de daad van afluisteren stelt, het volstaat dat hij een derde opdracht daartoe geeft. Bijvoorbeeld : een persoon was deelnemer aan de telecommunicatie en beschikt daar nu over. Artikel 314bis§2 bepaalt dat, ook al beschikt u over (wat de wet noemt) een wettig gemaakte opname (het e-mail berichtje in ons geval), u toch strafbaar bent als u het doorstuurt (er gebruik van maakt) met bedrieglijk opzet of met de bedoeling schade te brengen. U hebt zich bijvoorbeeld valselijk voorgedaan als een specialist m.b.t. relatie-problemen en u krijgt een berichtje waarin iemand u zijn slaapkamergeheimen uiteendoet. Als u dat nadien aan de grote klok zou hangen (doorsturen aan het hele bedrijf bv.) bent u dus strafbaar wegens het bedrieglijk opzet en uw bedoeling schade toe te brengen.

Tevens moet er rekening mee worden gehouden dat, indien de inhoud van de e-mail auteursrechtelijk beschermd is, toestemming van de auteur van de e-mail is vereist."

Het recht op eerbiediging van het privé-leven of van de privacy verleent het individu bescherming tegen het bekomen en verspreiden van persoonlijke informatie over hemzelf. Dit recht is een grondrecht dat omschreven wordt in artikel 22 van de Grondwet, artikel 8 van het Europees Verdrag ter Bescherming van de Rechten van de Mens en artikel 17 van het Internationaal Verdrag Inzake Burgerrechten en Politieke Rechten.

Kortom in de hoger vernoemde voorbeelden was het niet toegelaten dat persoon X een bericht van persoon Y doorstuurt naar persoon Z, zonder toestemming van persoon Y, wat ook de inhoud, opzet of aard van het bericht is. Zelfs al gaat het om racistische, bedreigende of seksueel obscene berichten, berichten die kwetsen of vernederend zijn. Men heeft niet het recht dit zomaar door te sturen. Men kan een ander persoon attent maken op een ongepast bericht, maar het bericht integraal doorsturen naar anderen of verspreiden via andere weg, zoals forums, blogs, facebook, enz. is door de wet verboden. Nu is er natuurlijk niets aan de hand bij onschuldige berichten met neutrale informatie. E-mailgebruikers moeten nu niet ongerust worden dat ze geen enkele e-mail mogen doorsturen. Maar wanneer de persoon die u een e-mail stuurt, schade zou oplopen hetzij professioneel of emotioneel-relationeel als u de mail doorstuurt dan bent u in principe strafbaar. Het hangt dus van je persoonlijk oordeel over de inhoud af of je het kan doorsturen of niet.

Daarom volgende belangrijke stelregels

-Stuur niet te snel e-mails door naar andere personen waaronder informatie van iemand anders staat. Deze persoon moet toestemming geven vooraleer je deze info doorstuurt want er stond niet expliciet in de mail dat deze info doorgestuurd mocht worden als dat aan jou werd gericht. Als je toch iets wil doorsturen, verwijder dan de info die onderaan de mail van de andere persoon vermeld staat of vergewis u ervan dat betrokkene door de informatie niet in diskrediet kan gebracht worden. Of beter vraag hem of haar toestemming of de mail doorgestuurd mag worden naar iemand anders. Dit geldt ook in arbeidscontext voor werkemailverkeer. Je bent schuldig aan schending van het briefgeheim indien je het toch doet.

- Het is niet toegelaten e-mailinformatie die niet aan jou gericht was, maar die je in de mail aantreft omdat die doorgestuurd was, aan te wenden voor gelijk welk doel. Nogmaals als je die info wil gebruiken, moet je eerst toestemming vragen van de oorspronkelijke schrijver van het bericht.

-Als je een systeem van kettingmails aantreft, waar telkens informatie wordt doorgestuurd. Verwijder dan de persoonlijke gegevens van alle betrokkenen vooraleer je het doorstuurt. Misschien was de info al aangepast en kan iemand van de personen die achter jou staat in de kettingmail ernstige schade oplopen als jij het doorstuurt. In principe kan je daarvoor strafbaar gesteld worden.
-Wees dus ook voorzichtig met het posten van e-mails van anderen in publieke fora zoals facebook, twitter , enz. zonder ook weer te vragen aan betrokkene of die info doorgegeven mocht worden.
-Gebruik je gezond verstand om te oordelen of je het mag doorsturen of niet.

<u>Registreren van e-mail/ e-mailverkeer loggen.</u>

Artikel 109terD van de Belgacomwet heeft betrekking op het kennis nemen, registreren, enz. van het bestaan van een telecommunicatiebericht of van gegevens over de communicatie, zoals de naam van de correspondenten, het tijdstip of de duur, zonder kennis te nemen van de inhoud ervan. Men hoeft niet zelf de inbreuk op artikel 109terD te plegen. Het volstaat dat met een dergelijke inbreuk pleegt door toedoen van een andere persoon. Artikel 109terD, 1° verbiedt het kennis nemen van het bestaan van telecommunicatieberichten. Het moet gaan om communicatie tussen minstens twee personen, waarbij de ene een boodschap doorgeeft aan de andere(n), en waarbij degene die registreert niet deelneemt aan de communicatie. Tenslotte moet er in hoofde van degene die registreert bedrieglijk opzet bestaan: de dader moet doelbewust de elektronische communicatie van anderen registreren, met het voornemen het geheim van het telecommunicatiebericht te doorbreken. Artikel 109terD, 2° bepaalt onder meer dat het verboden is met bedrieglijk opzet de andere persoon te identificeren. Het is dus verboden om na te gaan welke de oorsprong en de bestemming is van het telecommunicatiebericht. Het strafbaar karakter vervalt wanneer de dader de toestemming heeft van alle andere personen, die rechtstreeks of onrechtstreeks betrokken zijn bij de bedoelde informatie, identificatie of gegevens. Maar er zijn enkele uitzonderingen.

Het grondrecht op privacy is geen absoluut recht en het openbaar gezag kan er, weliswaar limitatieve, beperkingen aan stellen. Artikel 109terE van de Belgacomwet voorziet drie uitzonderingen, waarbij het afluisteren of het registreren van privé-communicatie wel toegelaten kan zijn. Bovendien moet de Wet inzake informaticacriminaliteit worden vermeld.

1. Wanneer de wet het toestaat of oplegt: het opsporings- en/of gerechtelijk onderzoek. Onder meer in het kader van een opsporings- en/of gerechtelijk onderzoek zijn er inbreuken mogelijk op het principieel tapverbod (inkijken of registreren van e-mail). In elk van deze gevallen geldt een medewerkingsplicht van de operatoren. Onder de strikte voorwaarden van artikel 90ter e.v. van het Wetboek van Strafvordering kan het afluisteren van privé-communicatie, dus ook inkijken van e-mailverkeer worden toegelaten. Deze echte tapmaatregel kan enkel door de onderzoeksrechter bevolen worden voor de duur van 1 maand, verlengbaar tot maximaal 6 maanden.

2. Wanneer het enig doel erin bestaat de goede werking van het netwerk na te gaan en de goede uitvoering van de telecommunicatiedienst te garanderen. Alle informatie, identificatie en gegevens die verkregen zijn op grond van dit tweede punt mogen ook uitsluitend om dezelfde redenen worden onthuld. Netwerkbeheerders mogen het principe van het telecommunicatiegeheim overtreden om de continuïteit van de telecommunicatiedienst te verzorgen. Hierbij geldt onverkort het proportionaliteitsbeginsel: slechts wanneer en in zoverre het nodig is om de dienst te verzorgen, mag de netwerkbeheerder bvb. kennis nemen van het bestaan of de inhoud van de telecommunicatieberichten. Tot de verzorging van de dienst behoren ook preventieve maatregelen, zoals het tijdelijk opslaan van een veiligheidskopie van elektronische postberichten. Bij voorkeur vraagt men wel toestemming van de eigenaar van de berichten, tenzij dat dit onmogelijk is.

3. Wanneer de handelingen worden gesteld om de interventie van hulp- en nooddiensten mogelijk te maken die antwoorden op aan hen gerichte verzoeken om hulp. Ook inzake de nieuwe wet inzake Informaticacriminaliteit worden een aantal nieuwe opsporings- en onderzoeksdaden in het Wetboek van Strafvordering ingeschreven. Het gaat hierbij om databeslag, netwerkzoeking en een bijzondere medewerkingsplicht, die alle drie een rol kunnen spelen in de strijd tegen het aanwenden van cryptografie voor criminele doeleinden.

Mogen systeembeheerders dan e-mail van gebruikers inkijken? In geval van problemen/klachten of wanneer een gebruiker om hulp verzoekt? Afgezien van de uitzonderingen, voorzien door Artikel

109terE van de Belgacomwet (o.m. indien nodig om de goede werking van het netwerk na te gaan en de goede uitvoering van de telecommunicatiedienst te garanderen), is het verbod om andermans communicatie in te kijken of te registreren principieel: de reden waarom men het e-mail bericht inkijkt of registreert is van geen belang. Of het nu gaat om eerbare doeleinden (bv. in geval van problemen of klachten) of met kwade bedoelingen, men blijft even strafbaar. De bepalingen zijn zeer neutraal opgesteld: zij bestraffen het pure afluisteren of registreren, zonder rekening te houden met de redenen van het afluisteren of registreren. Hetzelfde geldt bij overlijden van een student-werknemer. In geval van zelfmoord bvb, willen de nabestaanden graag de mailbox kennen van hun kind-werknemer om zo zijn beweegredenen te achterhalen. Ook hier blijven de aangehaalde regels onverminderd van kracht en men kan niet zomaar besluiten dat men rustig de mailbox van de overledene mag inzien. Men schendt dan immers de rechten van de anderen, die ook hun toestemming niet hebben gegeven (uiteraard kan een overledene geen toestemming meer verlenen). Slecht bij grote uitzondering kan hier van afgeweken worden, vb zelfmoordpoging, ernstig misdrijf, enz.

Kan een bedrijf, universiteit of ISP een overeenkomst (CAO, intern reglement, ...) sluiten met werknemers, studenten of klanten zodat e-mail wel mag ingekeken of geregistreerd worden?

In een arbeidsomgeving, op de universiteit of hogeschool, met een ISP kan een overeenkomst worden gesloten waarbij de werknemer -student-gebruiker zijn toestemming verleent. Daarmee is de zaak echter nog niet opgelost: men heeft zich nu enkel verzekerd van de toestemming van de eigen werknemers, studenten, klanten…. De toestemming van de communicatiepartner blijft nog vereist (tenzij deze eveneens verbonden is door deze overeenkomst). Zoals reeds werd uiteengezet, wordt de e-mail immers beschermd, tenzij alle betrokken gebruikers hebben ingestemd (Belgacomwet, Strafwetboek, Privacy Wet), m.a.w., indien zij allen afstand van hun bescherming hebben gedaan. De toestemming maakt dan een rechtvaardigingsgrond uit, waardoor de wederrechtelijkheid vervalt van een in beginsel strafbare handeling. De toestemming kan uitdrukkelijk, bijzonder maar ook stilzwijgend en uit een geheel van omstandigheden blijken. Ook al heeft men niet uitdrukkelijk en voorafgaand de toestemming van elke deelnemer aan de communicatie bekomen, toch kan deze geacht worden stilzwijgend te zijn bekomen of blijken uit het geheel van omstandigheden (bv. ketting-brieven, petitie).

Het is duidelijk dat aan deze voorwaarde (toestemming van alle betrokkenen) zelden of nooit voldaan zal zijn. Omdat deze toestemming vrijwel nooit verkregen zal kunnen worden, is controle van de elektronische post van de werknemers-studenten-klanten van ISP voor de werkgever-systeembeheerder praktisch uitgesloten. Enkel als een bedrijf, universiteit of ISP via bvb een overeenkomst de toestemming van hun gebruikers zou hebben bekomen, en de communicatiepartner is eveneens iemand van dat bedrijf, die universiteit of die ISP, die dezelfde overeenkomst heeft ondertekend (bvb alle interne E-mail van werknemers, studenten of ISP), dan zou aan deze voorwaarde voldaan zijn. Toch kan dit nuttig zijn.

Een concreet reëel gebeurd voorbeeld kan dit illustreren. Een student krijgt een onvoldoende op zijn examen omdat hij een werkstuk niet tijdig via e-mail heeft ingeleverd. De student beweert dat hij het wel tijdig verzonden heeft, maar de docent vermeldt dit nooit ontvangen te hebben. Met toestemming van de student én de docent analyseert men het e-mailverkeer uit de betrokken periode en uiteindelijk bleek dat de student de e-mail met de eindopdracht wel degelijk verstuurde en de docent het in zijn mailbox ontvangen had. Om een of andere reden had hij dit overzien of per ongeluk gewist, maar voor de student in kwestie betekende dit het grote verschil tussen slagen of niet slagen voor een vak én een academiejaar.
Een ander voorbeeld. In organisatie X behandelt secretaresse Y alle binnenkomende e-mails. Maar de dame valt zwaar ziek en ligt een tijd in coma door een ongeval. In dit geval mag de communicatie met de organisatie niet stoppen en kan het nodig zijn de e-mailbox toch te openen. Een goede raad aan organisaties is dan ook om e-mailcontacten met de buitenwereld niet aan één persoon toe te vertrouwen , maar aan een e-mailadres dat door meerdere personen geopend kan worden naargelang de behoefte. Zo vermijdt men het probleem dat e-mails voor langere periode niet opgevolgd kunnen worden en niemand er aan kan. Een goede archivering van e-mails in de organisatie met toegang van meerdere personen is in dit geval ook aangewezen om op langere termijn communicatie te kunnen opvolgen.

Het telecommunicatiegeheim (ook e-mail) is van openbare orde. Er is dus een vrij streng verbod op kennisname van inhoud en bestaan van (tele)communicatie. Maar voor de werkgever is dit verregaand verbod op zijn gezagsuitoefening niet steeds houdbaar. Het is dus wenselijk dat er zoals boven vermeld uitzonderingen zijn waardoor de werkgever toch inbreuken kan plegen op de privacy (weliswaar gereglementeerd) zonder steeds strafrechtelijk veroordeeld te worden.

Mogen logs van in- en uitgaande E-mail bijgehouden worden voor statistieken, voor accounting of om misbruik op te sporen?

Logging van in- en uitgaande mail is luidens artikel 109terD van de Telecomwet niet toegelaten. Logging zal enkel toegelaten zijn indien men toestemming heeft van alle betrokkenen, of indien men onder de in artikel 109terD voorziene uitzonderingen valt. Naast de principiële niet-toelaatbaarheid van logging van in- en uitgaande e-mail, is ook het inkijken van de logs niet toegelaten. Bovendien zal de Privacy-wet van toepassing zijn van zodra het om de verwerking van persoonsgegevens gaat. Anonieme gegevens, zoals die bijvoorbeeld voor statistische doeleinden worden verwerkt, zijn geen persoonsgegevens in de zin van de wet, echter slechts voor zover niemand - noch de verantwoordelijke, noch iemand anders - de identiteit van de betrokkene nog kan achterhalen. Persoonsgegevens zijn iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Dit is iedere persoon die direct of indirect kan worden geïdentificeerd aan de hand van een identificatienummer of van één of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit. Als de logging er bvb in bestaat bij te houden welke gebruiker (via een persoonlijke login en persoonlijk paswoord) op welk tijdstip, tot welk tijdstip op het netwerk was ingelogd en wat hij daar uitspookte, zijn dit dus persoonsgegevens. Er is daarentegen mogelijk geen sprake van persoonsgegevens als bvb een pc-klas tijdelijk publiek wordt geplaatst. Hiermee bedoelen we pc´s waarbij de gebruiker inlogt via een niet persoonsgebonden login (zoals het nummer van de pc) en zonder paswoord (ofwel met een niet persoonsgebonden algemeen paswoord.

Om misverstanden te vermijden verstuur je binnen organisaties privé-mails best vanuit een privé-emailadres en professionele mails vanuit je professionele adres. Het is ook aangewezen onder elke e-mail vanuit een professioneel adres te vermelden dat de e-mails opgeslagen, gelogd of zelfs ingekeken kunnen worden, zodat de afzender weet dat zijn reacties aan dit adres eventueel bij de werkgever bekend kunnen geraken, ook al is dit in principe door de wet verboden. Privé-emailverkeer mag door de werknemer niet ingekeken worden, die verstuur je dan ook liefst vanuit een voor de werkgever veiligere internetomgeving zoals Hotmail, Yahoo, of G-mail dus ook best niet via je outlook of andere emailprogramma waar je e-mailt met telenet of skynet. Als je die accounts via een website benadert is er geen probleem. Maar let op : in sommige arbeidscontracten staat expliciet dat er niet tijdens het werk privé op internet gesurft mag worden. Dan reserveer je dit soort mailverkeer maar voor thuis….

<u>Mag men e-mailgegevens verzameld vanuit verstuurde mails gebruiken</u> ?

Vele mensen hebben de onhebbelijke gewoonte om een bericht te versturen naar een grote groep mensen en die allemaal in de aanhef ‘Aan’ of ‘CC’ te plaatsen zodat iedereen ziet wie de betrokken e-mail krijgt, maar meteen ook alle e-mailadressen van alle betrokkenen kent en kan gebruiken. Zo kreeg ik zelf regelmatig mails van de sportclub van mijn kinderen met daarin tientallen e-mailadressen van ouders van andere kinderen. Ik heb zo al een heel bestand van e-mailcontacten opgebouwd door gewoon de e-mails te bewaren. Een bekende welzijnsorganisatie stuurde mij een mailing omtrent een bijscholing naar haar hele adressenbestand, zodat ik meteen beschikte over enkele honderden e-mailadressen van organisaties en werknemers in de welzijnssector die voor mij interessant waren om op mijn beurt te bewerken met interessante navormingsberichten. Mag dit zomaar : neen ! Het gebruik en de verspreiding van persoonsgegevens op het internet kan gevaren meebrengen voor het privéleven. Op diverse manieren worden persoonsgegevens op het internet verzameld en zonder dat we het beseffen, laten veel van onze activiteiten digitale sporen na. Een persoonsgegeven is elk gegeven (ongeacht zijn aard: tekst, beeld, geluid of andere) betreffende een natuurlijke persoon, die is of kan worden geïdentificeerd. De gegevens moeten dus kunnen worden gelinkt (zij het met redelijke moeite) met een identificeerbaar persoon. Indien niemand nog kan achterhalen op welke persoon de gegevens betrekking hebben, zijn het geen persoonsgegevens. Een e-mailadres met daarin de naam

van de persoon is een herkenbaar persoonsgegeven. Als deze persoonsgegevens op een (zij het gedeeltelijk) geautomatiseerde wijze, of op een niet-geautomatiseerde wijze (maar dan opgenomen in een bestand of bestemd om daarin te worden opgenomen) worden verwerkt en verspreid, is de wet toepasselijk. Een verwerking is eender welke handeling die men met persoonsgegevens verricht: gegevens verzamelen, opslaan, wijzigen, verwijderen, raadplegen, meedelen, gebruiken, verspreiden, enz. Het versturen naar een groot bestand en daarmee alle e-mailadressen van personen bekend maken is dus in principe strafbaar. Tijdens verkiezingen is het bijvoorbeeld verboden om e-mails met verkiezingspropaganda te versturen naar e-mailadressen van personen die je niet kent of waarmee je geen band hebt. Vreemd genoeg is brieven sturen wel toegelaten, maar mensen met e-mails bestoken om voor u of uw partij te laten stemmen is strikt verboden. Als een geadresseerde klacht indient, kan de kandidaat en zijn/haar partij daarvoor gesanctioneerd worden. Daarom een heel belangrijk advies. Plaats e-mailadressen die naar meerdere personen tegelijk verstuurd worden altijd in de rubriek 'BCC'! Zo kan men geen e-mailadressen onderscheppen en blijft de identiteit van de begunstigden geheim.

Mag men e-mails die van een gekend persoon komen altijd zomaar vertrouwen ?

Wanneer je een e-mail krijgt van een persoon vanuit een Hotmail, G-mail of Yahoo-adres kun je zowiezo altijd wantrouwen of dit bericht wel effectief van betrokken persoon komt. Iedereen kan immers onder eender welke identiteit heel gemakkelijk en snel een e-mailadres op het internet aanmaken zonder zijn of haar identiteit werkelijk bekend te maken. Wanneer dus een bedreigend of beledigend bericht komt van zulk een adres, beschuldig dan niet onmiddellijk de afzender van kwaadsprekerij. Het kan immers zo zijn dat iemand anders de mail verstuurde met de gekende identiteit. In principe kan je via de zogenaamde headers van e-mail wel nagaan vanuit welk IP-adres een bericht verstuurd werd, maar de e-mails kunnen ook verzonden zijn vanuit een school, een werksituatie waar meerdere mensen op dezelfde computer werken, een internetcafé, enz. Dit dus zeker niet te snel vertrouwen. Maar wat nu als de mail komt van iemand met een gekend en vast e-mailadres dat niet na te maken is. Ook dit is helaas makkelijk te omzeilen maar hier kan het nagaan van de headers van het bericht wel interessant zijn. Op de website www.shitzooi.nl kun je een anonieme mail versturen die komt vanuit een gekend e-mailadres, met eender welke vaste extensie, van het bedrijf, van telenet, belgacom, enz. In het voorbeeld ziet u hoe een e-mail werd verstuurd vanuit het privé-emailadres van Bart Dewever aan mezelf gericht. Voor alle duidelijkheid, het gaat om een totaal fictief nepbericht, door mezelf verstuurd vanuit betrokken website aan mijn e-mailadres. Met het voorbeeld wil ik zeker Bart Dewever niet in verlegenheid brengen maar gewoon aantonen dat je e-mails, zelfs al komen ze van betrouwbare personen met hun gekende e-mailadres, altijd heel kritisch moet onderzoeken, zeker als ze info bevatten die jou vreemd overkomt. Je kunt via de headers van het bericht nagaan of het echte dan wel nepberichten zijn. Op de website www.cyberpesten.be vind je meer info over hoe je deze headers kan raadplegen.

We willen deze bijdrage over e-mailetiquette eindigen met enkele algemene praktische regels.

Met spreekt in dit kader ook wel van 'netiquette. Dit is een samentrekking van de woorden 'netwerk' en 'etiquette': het omvat een aantal richtlijnen voor het gebruik van internet en e-mail. De meeste gedragsregels voor het internet liggen nogal voor de hand. Toch vergeten sommige internetgebruikers wel eens dat ze via het netwerk met mensen communiceren en niet met machines. Bij communicatie via het netwerk is aanvullende communicatie in de vorm van gezichtsuitdrukkingen, bewegingen en gebaren haast altijd afwezig. Dat maakt dat een boodschap soms anders overkomt dan bedoeld was. Verkeerd gebruik van dit medium kan ook voor veel frustraties bij andere internetgebruikers zorgen. De meeste problemen die je als gebruiker veelal zelf kunt voorkomen hebben betrekking op:

Te lange regels
Stel de maximale regellengte in op 70 tekens of minder. Hierdoor zal de tekst ook na een reply, waarbij er > voor jouw tekst gezet wordt, nog goed leesbaar blijven op de beeldschermen van de meeste gebruikers.

HTML in plaats van gewone tekst
In veel moderne e-mailprogramma's kun je instellen of je berichten met HTML ("met opmaak") of als

gewone tekst wil versturen. Kies bij voorkeur voor gewone tekst, HTML zorgt voor onnodige overhead. Je weet immers niet of de ontvangers van jouw bericht wel met HTML overweg kunnen

Bijlagen
Vermijd het doorsturen van zeer volumineuze bestanden. Sommige e-mailproviders leggen trouwens een maximumgrens op , maar denk ook aan hen die met een minder snelle internetverbinding werken. Een bijlage van 25 Mb kan al vlug 5 tot 10 minuten aan internetverkeer kosten bij een trage verbinding.

Duidelijkheid
Een elektronische brief is niet veel anders dan een gewone brief. Gebruik een passende aanhef en ondertekening en geef in de onderwerpregel (subject) duidelijk aan waar het bericht over gaat. Omdat veel mensen op grond van het onderwerp hun e-mail archiveren is het vaak beter om per onderwerp een (korter) mailtje te sturen in plaats van een lange mail met diverse verschillende onderwerpen. Ondertekenen je berichten altijd met de volledige naam én je persoonlijke gegevens zodat de afzender weet van wie de e-mail komt. Gebruik bij voorkeur een handtekening, die standaard automatisch onder elke e-mail komt.

Emoties
Omdat 'lichaamstaal' in netwerkcommunicatie ontbreekt, valt het gebruik van humor, ironie of sarcasme vaak niet mee. Lees een emotioneel geladen tekst in ieder geval nog eens door alvorens deze te versturen. Bedenk dat een eenmaal verstuurd bericht niet meer kan worden teruggehaald…Eventueel kan je een bepaalde emotie aangeven met de zgn. smiley's bijvoorbeeld blij :-) droevig :-(enz.

Controle
Verifieer regelmatig de inkomende post. Een bericht niet openen is onbeleefd en bovendien vervelend voor de verzender. Antwoord tijdig op de berichten en informeer de afzender welk gevolg je zult geven aan zijn bericht. Gebruik het attribuut "dringend" alleen als het absoluut noodzakelijk is. Vermijd het systematisch gebruik van de leesbevestiging. Overdrijf dan ook wel niet in het antwoorden. Als je iemand iets vraagt en die antwoordt dat hij het zal onderzoeken, antwoordt dan niet nog eens met een dankjewel voor het onderzoeken, dan zit je in een rondje te mailen en dat is overbodig, maar binnen een redelijke termijn antwoorden op een vraag of reactie is een elementaire vorm van beleefdheid, ook al gaat het om je baas, departementshoofd, collega, enz….

Mailing list
Een mailing list komt overeen met een inschrijving bij een informatieleverancier (news server voor het automatisch en regelmatig verkrijgen van informatie). De gebruiker bewaart van alle mailing lists een bewijs en de instructies om die inschrijving te annuleren. Schrijf bij voorkeur niet in op uitgebreide mailing lists om overbelasting of blokkering van de mailboxen te vermijden.
Stuur nooit reclameachtige boodschappen naar vele mailinglijsten en nieuwsgroepen tegelijk. Dit wordt door de meeste internetgebruikers gezien als 'spam (ongewenste e-mail).

Spam
Reageer bij voorkeur niet op e-mails die van spamservers komen. Vaak tref je bij die ongewenste reclameberichten onderaan een link waar je je kan uitschrijven. Als het gaat om een dienst waar je zelf voor ingeschreven hebt, werkt dit meestal wel goed om je terug uit te schrijven, maar als het gaat om ongewenste post, kan je beter jezelf niet uitschrijven. Computerprogramma's zoeken permanent op het internet en onbeschermde e-mailservers naar bruikbare e-mails om je ongewenste reclame te verzenden. Als iemand reageert en zich wenst uit te schrijven is dit een signaal voor de spammer om aan te geven dat het een bestaand e-mailadres is en dat de afzender deze berichten ook opent en leest. Je mag er gegarandeerd zeker van zijn dat je nog veel meer van dit soort ongewenste berichten gaat krijgen. Reageer dus best niet en probeer de afzender te blokkeren, hoewel de meeste spammers dit weten en telkens nieuwe e-mailadressen gebruiken. Moet je een e-mailadres opgeven om software te kunnen downloaden, iets te kunnen lezen, enz. Gebruik dan een snel aanmaakbaar onschuldig hotmail of ander adres, dat je daar alleen voor gebruikt. Als je in die mailbox teveel spam aantreft, maak je een nieuwe account aan, tot die weer volslipt…

E-mailen… een kunst

Deze tips gaan niet over de mailtjes die je stuurt naar vrienden en vriendinnen, daar bemoeien we ons niet mee. Ze gaan wel over het iets formelere e-mailverkeer: mails naar collega's op het werk, docenten, werkgevers, bedrijven, stagementoren enz…

NIET ZO	MAAR ZO
Stuur geen videoclips, grappen, kettingbrieven enz…	Stuur simpele, ondubbelzinnige boodschappen
Afzender: rupsebolleke@hotmail.com	Gebruik een duidelijk, professioneel e-mailadres waarin je eigen naam zit.
"Kunt ge ff uw notas missen?"	Correcte taal en spelling, geen SMS-taal
"Subject: klacht"	Duidelijke, kernachtige onderwerpzin: b.v. "Subject: stagereflectie 25 maart"
Subject: RE:RE:RE….	Liever geen kettingreacties, pas je onderwerpregel aan
Aanspreking: "Hoi"	"Geachte heer/mevrouw (naam)" "Beste/Dag mijnheer/mevrouw (naam)"
Lange aanloop	Structureer de informatie: begin met het belangrijkste (beeldscherm is immers klein)
Geen ondertekening, afzender dus onbekend, want wie is in godsnaam 'Rupsebolleke"????	Maak een aparte handtekening voor formelere mails, eventueel voorafgegaan door een slotformule als "Met vriendelijke groeten". Die kun je dan telkens invoegen als je die nodig hebt. Snel en gemakkelijk!
Lege mail met een bijlage	Maak een begeleidend briefje bij je bijlage.
Titel bijlage: "klacht.doc"	Geef het document in de bijlage een duidelijke naam: je eigen naam/organisatie/duidelijke titel van het document enz. b.v. "Johan Peeters stagereflectie november"
"Oeps…bijlage vergeten, hier komt ie dan…"	Controleer of de bijlage er werkelijk bijzit. TIP: voeg de bijlage éérst toe, voor je aan het tekstvak begint.

En tenslotte een heel belangrijke gouden raad : Think before you click ! Dit wil zeggen : als je een e-mail krijgt die je opwindt of je wil reageren op iemand of iets, verstuur de e-mail dan niet meteen, maar sla hem op in je concepten en denk er later nog eens over na. Het grote gevaar bij e-mails is dat ze je de kans geven om onmiddellijk te reageren, direct zonder veel te moeten nadenken, maar zo gauw als de mail verstuurd is, is hij niet meer terug te halen en bestaat zelfs het risico dat die ontelbare malen door anderen wordt verder gestuurd. Als je dus boos of verontwaardigd bent en je kunt je niet inhouden….schrijf een brief, dat vraagt wat meer tijd vooraleer je hem op de post doet, trek de internetstekker uit, ga joggen, uitwaaien, ontspannen, enz. en wacht even met reageren. Vaak heb je achteraf spijt dat je te snel op het knopje 'verzenden' hebt geklikt.

Meer info over netiquette: zie ook http://web.inter.nl.net/users/Maurice.Makaay/

Gerard Gielen