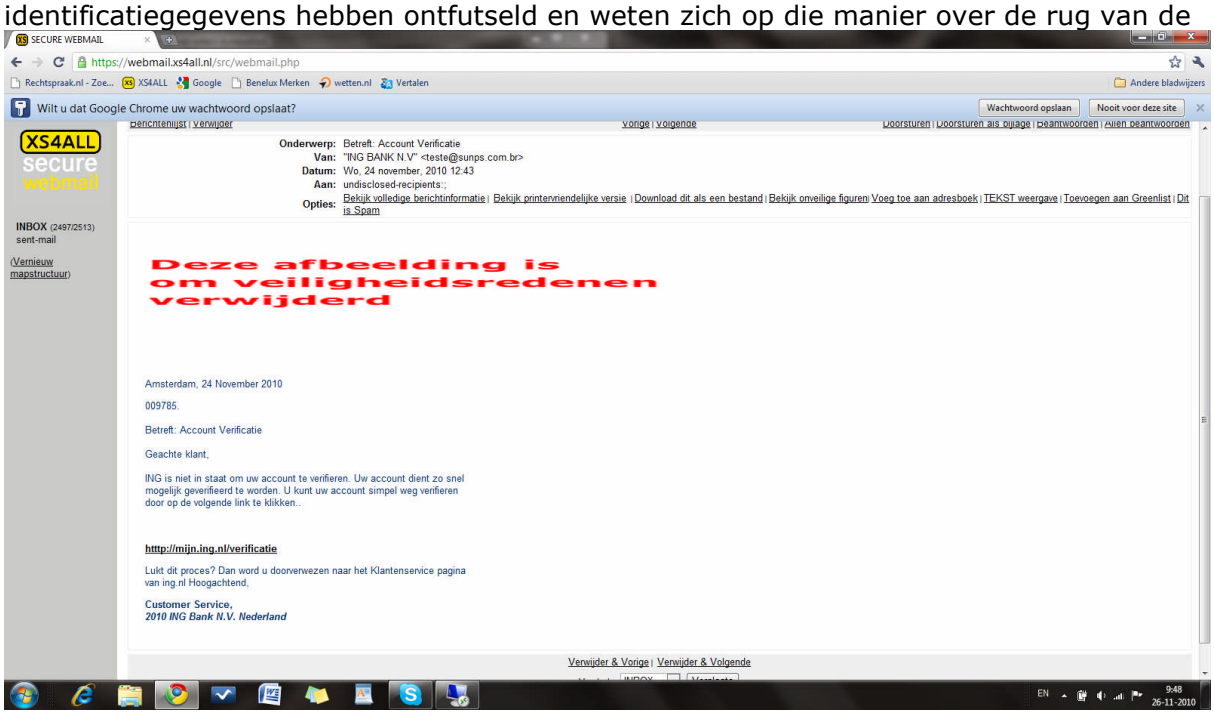
Zorgverplichtingen ISP's tegen internetcriminaliteit

De gevaren van deelname aan het internetverkeer zijn legio. ISP's, internetservice providers zoals Planet.nl, Xs4all zijn wettelijk verplicht om hun abonnees in bepaalde mate te beschermen tegen internetcriminaliteit.

De gevaren van internet of beter gezegd internetgebruik zijn onder te verdelen in Botnets, identiteitsfraude en computerinbraak.

Botnets zijn netwerken van besmette computers, ook wel "zombies" genaamd, die bestemd zijn voor het massaal en ineens versturen van spamberichten of het uitvoeren van cyberaanvallen, zgn. DDoS [Distributed Denial of Services]-aanvallen. Een DDoS-aanval is het pressiemiddel om iets gedaan te krijgen, bijv. een (meestal kapitaalkrachtig) bedrijf af te persen. DDOS-aanvallen zijn bedoeld om de servers van het slachtoffer te laten crashen. Het slachtoffer is meestal een bedrijf voor wie haar ononderbroken internetconnectie gevoelig ligt. De afweging die het afgeperste slachtoffer meestal zal maken is eerder calculerend dan emotioneel; het aan de boeven te betalen bedrag is meestal (aanzienlijk) lager dan de schade die dat bedrijf zal oplopen als haar servers door een overload van verbindingsverzoeken (de DDoS-aanval) zullen worden platgelegd. Het vervelende van botnets is dat de computereigenaar zich van geen schuld bewust is, terwijl zijn PC ongenood aan een crimineel netwerk deelneemt. Hij of zij heeft pas in de gaten dat zijn/haar PC een "zombie" is, als de politie op basis van het IP-adres zijn of haar identiteit heeft achterhaald en is langs geweest om de computereigenaar aan de tand te voelen.

Bij identiteitsfraude gaat het in vrijwel alle gevallen om een sluwe manier om de identiteitsgegevens van de minder oplettende internetgebruiker te ontfutselen. De boeven zijn dan op jacht naar diens gebruikersgegevens van zijn/haar internetbank of webshop m.a.w. zijn inlognaam en wachtwoord. De boeven doen zich dan bij de internetbankier of bij de webshop voor alsof ze de persoon zijn van wie ze de identificatiegegevens hebben ontfutseld en weten zich op die manier over de rug van de



internetgebruiker te verrijken. *Phishing*, het vissen naar ID-bankgegevens gebeurt meestal door een vals e-mailbericht aan de internetgebruiker te sturen. In dat bericht dat afkomstig lijkt te zijn van de internetbank, wordt gevraagd om verder te klikken en op een website, die wederom sprekend lijkt op die van de echte bank, inlognaam en wachtwoord in te typen. Meestal staan er in Phishing e-mails dusdanige rare

mededelingen en spellings- en grammaticale fouten dat bij de internetgebruiker toch allerlei bellen zouden moeten afgaan. Maar, sinds de eerste Postbank Phishing uit 2004 (al) is phishing een succesvolle methode gebleven. Waaruit ik maar wil concluderen dat boeven er taalkundig niet op vooruit zijn gegaan en er nog altijd internetgebruikers zijn die niet kunnen lezen of vreselijk goedgelovig of naïef zijn.

Tegen phishing kunnen providers geen technische maatregelen treffen, behalve dat phishing mails als spam worden onderschept en daarom in de spambox van de abonnee terechtkomen of automatisch worden verwijderd, afhankelijk van de instellingen van de abonnee.

Andere beproefde methode om online ID-gegevens te ontvreemden is door middel van malware, het acroniem van *malicious software*. De internetgebruiker heeft dan bewust of onbewust zijn PC laten infecteren met ongenode software die tot functie heeft inloggegevens in de computer op te sporen en aan de boeven te versturen.

Het derde gevaar is *hacking* oftewel computerinbraak. Computervredebreuk ook wel genaamd, is bij wet, artikel 138a wetboek van strafrecht, verboden, maar het is geen sinecure om de hackers op te pakken. Het spoor naar de boeven loopt meestal ergens ver buiten de EG-grenzen dood. Af en toe wordt er succes geboekt tegen een vaak wat dommere hacker (slimme hackers laten immers geen sporen na en houden aan de borreltafel hun mond). Op 2 maart 1995 heeft de arrondissementsrechtbank te Utrecht een 22-jarige man veroordeeld tot een geldboete van fl. 5.000 en een voorwaardelijke gevangenisstraf van zes maanden voor het plegen van computervredebreuk. De man had kans gezien om zonder toestemming binnen te dringen in computers van een vijftal universiteiten, een bedrijf in Venlo en een aantal instellingen in IJsland en de Verenigde Staten.

Op grond van de Telecommunicatiewet (artikel 11.3 Tcw) zijn ISP's verplicht om technische en organisatorische maatregelen te treffen ter bescherming tegen internetcriminaliteit. Dat betekent dat de hardware en software van de computersystemen van de ISP zodanig moet zijn gebouwd en ingericht dat daardoor op technische wijze een inbreuk kan worden voorkomen. Technische vereisten zijn voortdurend in beweging. Die worden voortdurend strenger, omdat de technische kennis en mogelijkheden evolueren. Dus, een beveiliging die tien jaar geleden afdoende was volgens de standaarden toentertijd, zal zonder meer nu ondermaats zijn; de veiligheidsnormen liggen tegenwoordig een heel stuk hoger.

Een ISP kan dus door een beschadigde abonnee civielrechtelijk worden aangesproken op het feit dat de ISP onvoldoende technische maatregelen heeft getroffen. Verder dienen ISP's er voor te zorgen dat zij voldoende informatie aan hun abonnees ter beschikking stellen, zodat die een inschatting kunnen maken van de risico's die ze lopen door gebruik te maken van de internetdiensten van de ISP. Het gaat meer bepaald om risico's van spam, virussen die via de ISP de abonnee kunnen bereiken en wat de abonnee zelf kan doen om die risico's te minimaliseren. Verder moeten de ISP's hun abonnees informeren over de maatregelen die zijzelf kunnen nemen ter voorkoming (zoveel mogelijk) van ongemak.

Op de ISP's rusten dus inspanningsverplichtingen van technische, organisatorische en informatieve aard. Xs4all bijvoorbeeld stelt een checklist ter beschikking waarvan een veiligheidspakket, updates, beveiligingsmodaliteiten en keuze wachtwoord onderdeel van uitmaken. Ook waarschuwt die provider voor nepmails (phishing).

15 juli 2010, mr. F.J. Van Eeckhoutte, ICT/IE & Corporate,
www.vaneeckhoutteadvocaten.nl