

## Gummen kan op internet niet

19-02-2010 13:07 | tekst Gijsbert Bouw



### **Digitale veiligheid is een illusie. Ondanks alle pogingen om het internet veilig te krijgen, nemen diefstal, vernielingen en afpersingen alleen maar toe. Voorzichtig zijn lijkt de beste oplossing, hoe voor de hand liggend ook.**

Gevaren zijn er online legio. Neem de vrijgezel die tuitert dat hij aan het werk is op kantoor. Iedereen die dat leest en kwaad wil, kan ondertussen inbreken in zijn huis.

Of neem de frivole student die foto's van een feestje van zijn studentenvereniging op zijn Hyvesprofiel zet, waar te zien is dat hij een slokje te veel heeft gedronken. De directeur van het bedrijf waar hij na zijn studie solliciteert, ziet de foto's en kiest wellicht liever een andere kandidaat.

Of neem de Roemeense bende die contact zoekt met Nederlandse, zestienjarige jongens en hen 300 euro per maand betaalt. De kereltjes moeten één ding doen: Via Hyves goede contacten leggen met bemiddelde Nederlanders en bij hen lospeuteren wanneer ze op vakantie gaan. De bende haalt dan het huis leeg.

Onveilige situaties liggen om de hoek. En dan gaat het nog niet eens over virussen, skimmers, hackers, spam, spyware, rondslingerende usb-sticks en identiteitsdiefstal.

Dat internet onveilig is, is geen nieuws. Wel opmerkelijk is de houding van internetters. De meeste jongeren maken zich geen zorgen over digitale veiligheid, aldus Andy Clark, deskundige op het gebied van internetveiligheid. „We zijn niet zo geneigd ons veilig te gedragen. We gebruiken vaak één password met de naam van onze hond of onze achternaam. En we schrijven ze soms ook nog op.”

De opkomst van sociale netwerksites als Hyves en Facebook hebben de digitale onveiligheid alleen maar vergroot. Dat bleek begin deze maand uit onderzoek van G Data, een bedrijf dat is gespecialiseerd in online veiligheid. In de tweede helft van 2009 waren netwerksites steeds vaker doelwit van cybercriminelen. Soms om de controle over een persoonlijke pagina over te nemen, soms om accounts te gebruiken om virussen te verspreiden en soms om persoonlijke informatie van gebruikers te stelen om identiteitsfraude te plegen. G Data verwacht ook voor 2010 dat het aantal aanvallen op dergelijke netwerksites zal blijven toenemen.

Wie denkt dat de digitale criminaliteit weinig voorstelt, heeft het bij het verkeerde eind. Binnenkort gaat er in die vorm van misdaad meer geld om dan in de drugshandel, zegt Wilfred van Roij, directeur van recherchebureau Com-Connect. Optimistisch over de veiligheid op internet is hij niet. Zelfs over online bankieren is hij negatief gestemd. „Het lijkt wel veilig, maar is het niet. Banken vergoeden netjes alle schade die klanten oplopen door criminelen die online hun rekening hebben geplunderd. Dat doen ze om imago- en reputatieschade te voorkomen.”

Van Roij verbaast zich erover hoeveel persoonlijke gegevens en foto's gebruikers van Hyves en Facebook op hun profiel plaatsen. „Het is me een volkomen raadsel waarom dat gebeurt. Niet doen dus. Hackers zijn dol op zoveel persoonlijke gegevens. En gummen is op het internet niet mogelijk.”

Van Roij adviseert Hyvespagina's af te schermen voor vreemden. „Dat geldt ook als een leuk, twintigjarig meisje zich meldt. Het zou niet de eerste keer zijn dat een crimineel zich verschuilt achter een niet-bestaande identiteit.”

Een panklare oplossing voor het probleem van digitale onveiligheid is moeilijk te vinden. Van Roij: „Ik wil mensen zich ervan bewust maken dat veiligheid geen vanzelfsprekendheid is.”

Voorzichtig zijn met het plaatsen van persoonlijke gegevens op internet, garandeert geen volledige digitale veiligheid. Ook anderen kunnen gevoelige informatie over jou online plaatsen. Van Roij heeft een tip: „Houd met Google Alert bij waar je naam op het internet opduikt. Dan ben je in elk geval op de hoogte van wat er over je wordt gezegd.”

Het technische beveiligen van computers en digitale systemen is belangrijk. Maar de mens blijft de zwakste schakel in de digitale veiligheid, stelt Van Roij. Zestig procent van de problemen zou door de mens zijn veroorzaakt: kwijtraken van usb-sticks, stelen van bedrijfsgevoelige informatie en inbreken in computersystemen.

Van Roij: „Bedrijven gaan in de toekomst hun werknemers steeds meer volgen, verwacht ik. Ook is het voor ondernemingen raadzaam een internet- en e-mailprotocol te hebben, waarin staat hoe werknemers zich online moeten gedragen. Elke twee jaar moet die worden aangepast. Twitter hoort er ook in te staan.”

---

### **Informatie op oude pc's**

Niet alleen de computer op het bureau kan slachtoffer zijn van criminaliteit. Ook de afgeschreven variant biedt kwaadwillenden vaak veel persoonlijke informatie.

Digitaal recherchebureau Com-Connect onderzocht 36 tweedehands computers die het opkocht via veilingssites en ict-bedrijven.

Op de computers stonden bijna 1 miljoen bestanden. Op ruim een kwart van de pc's stonden alle bestanden nog, bijna de helft van de apparaten was geformatteerd.

De computers bevatten creditcardgegevens, inloggegevens van webwinkels, foto's en medische gegevens. Eén van de harde schijven was eigendom geweest van een advocate, waarop onder meer strafdossiers van cliënten stonden.

Bedrijven en personen moeten zich bewust zijn van wat ze op de pc achterlaten, zegt Van Roij van Com-Connect. „Formateren is niet afdoende. Wipen helpt wel: met een speciaal programma kun je bestanden definitief wissen van harde schijven.”

Niet alleen op pc's blijft informatie achter, ook op afgedankte mobieltjes staan sporen. Zeker nu een mobiele telefoon steeds meer op een kleine computer gaat lijken.