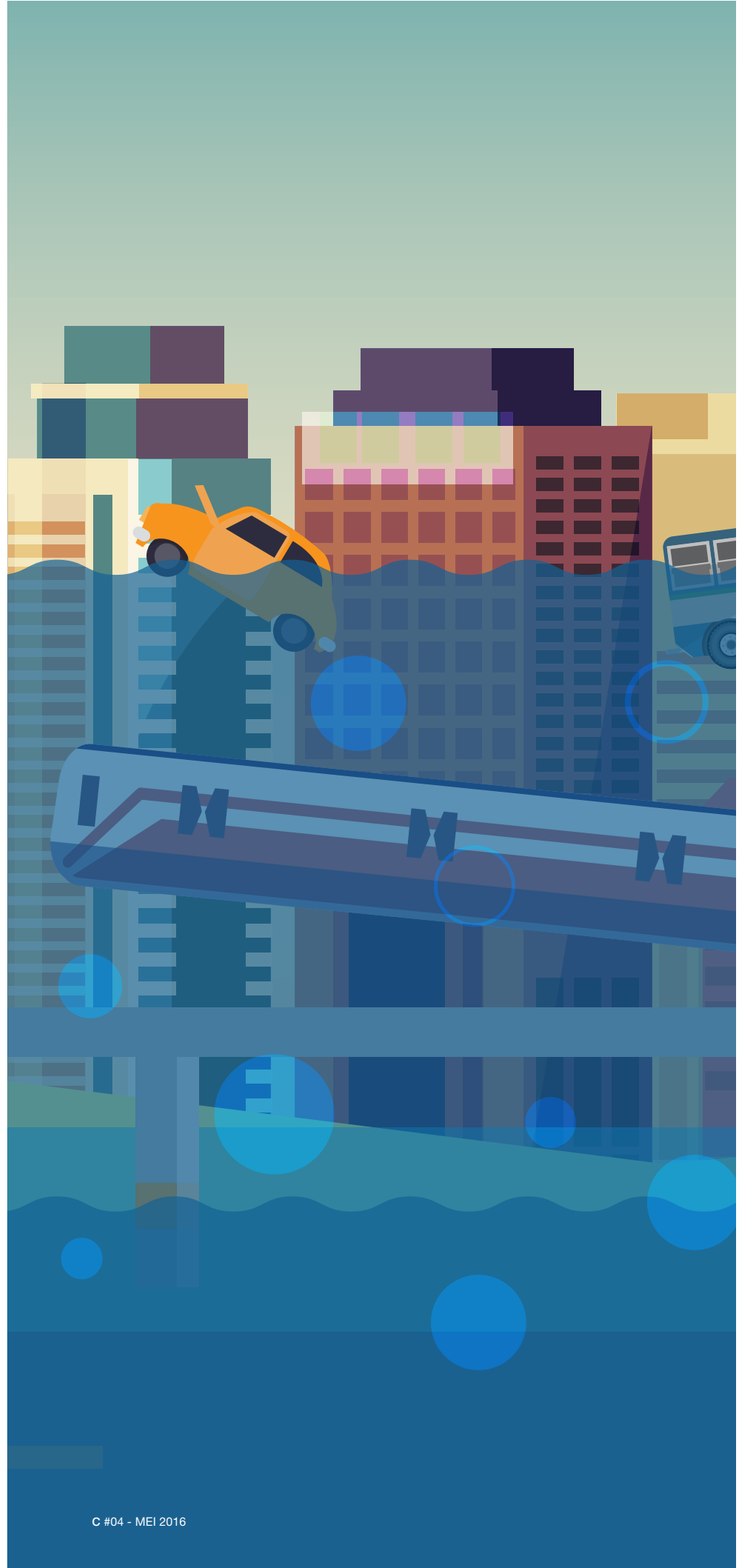
We lopen anno 2016 net zoveel en waarschijnlijk zelfs meer kans om slachtoffer te worden van digitale misdaad dan van fysiek geweld. Wordt bijvoorbeeld het systeem gehackt dat de bediening van sluizen regelt, dan kan dat een watersnood veroorzaken die het halve land onder water zet. Als kwaadwillenden er in slagen de digitale beveiliging van banken te kraken, kan dat een financiële crisis ontketenen. Zijn we voldoende toegerust om dergelijke bedreigingen het hoofd te bieden?

De burger en de strijd tegen cybercrime

Auteur
Bert Pol
redacteur C, vennoot van Tabula Rasa, verbonden aan de afdeling communicatiewetenschap van de Universiteit Twente en de afdeling psychologie van de Universiteit van Maastricht

Wim Kuijken, behalve Deltacommissaris ook bestuursvoorzitter van het nationale veiligheidscluster The Hague Security Delta (HSD), wees onlangs op de noodzaak 'dat de nationale politie nieuwe expertise aanboort om de digitale veiligheid te waarborgen. Daar is een andere manier van denken en handelen voor nodig.'[1]

Cybercriminaliteit is niet alleen een zaak van de politie: het gedrag van individuele burgers speelt ook een rol bij het voorkomen ervan. Privécomputers kunnen namelijk zonder dat we dat in de gaten hebben deel gaan uitmaken van een *botnet*, een netwerk van computers dat ingezet wordt voor criminele doeleinden. Als je dat weet, kun je er iets tegen doen. Bijvoorbeeld de instructies opvolgen die de Consuwijzer biedt op haar website (zie tiny.cc/qs31ay). Maar dat veronderstelt vanzelfsprekend dat je *weet* dat dit speelt. Dus dat je in elk geval enige kennis van zaken hebt en in staat en gemotiveerd bent actief op zoek te gaan naar dergelijke informatie.
Datzelfde geldt voor het voorkomen dat je slachtoffer wordt van phishing, virussen en misleidende mails waarmee ons wachtwoorden wordt ontfutseld die toegang geven tot onze bankrekeningen. Ook hier geldt: informatie en instructies zijn er wel. Diverse partijen hebben voorlichtingsmateriaal ontwikkeld dat laat zien waar we op moeten letten en wat we moeten doen. Zo is een schat aan informatie te vinden op https://veiliginternetten.nl, een initiatief van diverse ministeries en het bedrijfsleven. Ook KPN schenkt in haar nieuwsbrieven regelmatig aandacht aan digitale veiligheid. En de gezamenlijke banken lanceerden dit jaar twee tv-spots (tiny.cc/lu31ay en tiny.cc/7u31ay).



Gedrag en gemak

Dat zijn uitstekende initiatieven. Maar is het voldoende dat informatie beschikbaar is? Mensen moeten die informatie niet alleen weten te vinden, ze moeten die ook willen gebruiken. Een van de knelpunten is dat internet juist vanwege het gemak wordt gebruikt: je hoeft tegenwoordig niet meer de deur uit om aankopen te doen, je bankzaken te regelen, de onderhoudsbeurt voor je auto af te spreken. De tijd die zo vrijvalt, vullen we in ons drukke leven weer in met andere activiteiten. Als je je veilig wil gedragen op het internet, moet je zelf actief op zoek gaan naar informatie en allerlei handelingen uitvoeren. Daar moet je dan weer tijd voor vrijmaken. En dat gaat ten koste van de tijd en het gemak die we juist gewonnen hadden door het gebruik van internet.[2] Langetermijnvoordelen leggen het doorgaans af tegen kortetermijnnadelen.
In dergelijke situaties steekt ook het fenomeen onrealistisch optimisme al snel de kop op: 'Het zal toch allemaal zo'n vaart niet lopen?'[3] Campbell et al (2007) zagen in hun onderzoek dat degenen die vaak van internet gebruik maakten ook optimistischer waren, in die zin dat ze dachten dat zij minder kans op problemen maakten dan anderen. Hoe langer het goed gaat, hoe optimistischer velen kennelijk worden. Tot die conclusie komen ook Whitty et al (2015).[4] Zij constateerden in hun onderzoek ook dat kennis van de risico's alleen niet voldoende is om mensen af te houden van het delen van wachtwoorden: individuele verschillen spelen ook een rol. Zo blijken jongeren vaak wachtwoorden te delen. Maar ook mensen die er gevoelig voor zijn wat anderen van hen vinden: mogelijk zijn ze bang om uit de toon te vallen. ›

Ouderen en lager opgeleiden

Ouderen vormen een andere risicogroep, stellen Grimes et al (2010). In hun onderzoek bleken ouderen zich minder bewust van de gevaren, waarschijnlijk omdat ze nog zo weinig digitale ervaring hadden dat ze geen idee hadden van de risico's die eraan kleven. Naarmate het gebruik van internet toeneemt, groeit bij hen vaak ook het bewustzijn van de gevaren. Zij hebben daarom vooral baat bij cursussen en workshops.[5]

Een aparte groep vormen lager opgeleiden. Adolescenten uit lager opgeleide milieus blijken vaker riskant digitaal gedrag te vertonen.[6] Een verklaring daarvoor geven Van Deursen & Van Dijk (2014): lager opgeleiden gebruiken internet meer voor sociale interactie en spelletjes. Informatie over gevaren van onoplettend internet- en mailgebruik komt daardoor bij hen niet aan.[7]

Remedies

Er is dus nog werk aan de winkel om mensen kennis bij te brengen over de risico's van onoplettend mail- en internetgedrag. En om hen te *motiveren* relevante informatie op te zoeken en hen ertoe te bewegen die informatie ook te gebruiken om afdoende maatregelen te nemen. Dat is niet zo eenvoudig, omdat mensen die informatie snel en goed kunnen opzoeken, zich daarvoor niet zo snel de tijd zullen gunnen. Een ander deel van de mensen heeft moeite informatie te begrijpen. En niet zelden ook met informatie vinden. Natuurlijk zijn er remedies, maar daarvoor zal de buidel getrokken moeten worden. Het probleem lijkt ernstig genoeg om dat ook daadwerkelijk te doen. Zo doen Labuschagne (2011) en L.P. Beltran, M. Merabti en Q. Shi (2012) de suggestie veilig gedrag te stimuleren door spellen waarmee gebruikers op sociale netwerksites hun kennis kunnen testen. Of dat zal werken, zal moeten blijken.

Het lijkt een goed idee participatief onderzoek uit te voeren. Dat wil zeggen met mensen uit de doelgroepen na te gaan waar de knelpunten en kansen liggen en welke interventies kans van slagen hebben om *met* hen manieren te ontwikkelen om de digitale veiligheid in zo breed mogelijke lagen van de bevolking een forse impuls te geven.

Communicatieve interventies lijden vaak aan het manco dat ze worden ontwikkeld door hoger opgeleiden. Tunnelvisie lijkt dan bijna onvermijdelijk. Het gevolg is een zeer selectief bereik en effect van de interventies. ●

Literatuur

1. Het *Financieele Dagblad*, maandag 18 april 2016
2. Beltran, L. P., Merabti, M., & Shi, Q. (2012). The Use of a game-based interface for home network security. *13h Annual Postgraduate Symposium on Convergence of Telecommunications, Networking and Broadcasting* (PGNet 2012).
3. Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. *Computers in Human Behavior*, 23(3), 1273-1284.
4. Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior, and Social Networking*, 18(1), 3-7.
5. Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of Internet hazards. *Educational Gerontology*, 36(3), 173-192.
6. Notten, N. (2013). Risicogedrag en het wereldwijde web - De invloed van gezin en samenleving op het online risicogedrag van adolescenten vanuit een Europees perspectief. *Mens en maatschappij*, 88(4), 350-374.
7. Deursen, A. J. van, & Dijk, J. A. van (2014). The digital divide shifts to differences in usage. *New Media & Society*, 16(3), 507-526.