Ik kreeg een mailtje van <vul hier een willekeurige fake-id in>
Volgens de schrijver hadden hackers ingebroken in mijn PC en stiekem videoopnames van mij gemaakt op een moment dat je dat liever niet hebt.
Ik moest er wel om lachen. Het mailtje ziet er plausibel uit als je niks van computers weet. Of van mij. Of van mijn niet-bestaande web-cam….

“Even kijken om welk password het gaat….”
LinkedIn.

Dat was het dus. In 2012 is de slecht beveiligde website van LinkedIn gekraakt en is de password-database buitgemaakt. En de hackers zijn er in geslaagd de encryptiemethode die LinkedIn gebruikt heeft te kraken. En omdat die methode hetzelfde was voor alle passwords hadden de hackers daarna een lijst met miljoenen passwords en e-mail adressen, waaronder die van mij.
Helaas voor de hackers gebruik ik nooit op meer dan één plek hetzelfde password.
En LinkedIn heeft iedereen gedwongen een nieuw password te kiezen toen ze de hack ontdekten, dus je kan ook niet namens mij een bericht versturen via LinkedIn.

LinkedIn had zijn gegevens ook beter moeten beveiligen. Zelfs mijn doe-het-zelf WordPress website heeft een betere beveiliging.

Een paar weken geleden heb ik trouwens wel een webcam aangeschaft, die ik misschien nog een keer ga gebruiken voor het maken van een Youtube (nog zo’n perfect beveiligde website) video.
Een van de features van het ding is een klepje dat je dicht kan doen.