2 dagen geleden

Om iemands identiteit te stelen, hoef je geen hacker of meesteroplichter te zijn. Je kunt ook terecht bij de copyshop. Achteloze klanten veroorzaken daar zelf hun eigen privacylek. Gastcorrespondent Maaike Goslinga ging op onderzoek uit.

Een rondje copyshops leert: de grootste vijand van onze privacy zijn we zelf

Correspondent Data & Transparantie

Dimitri **TOKMETZIS**

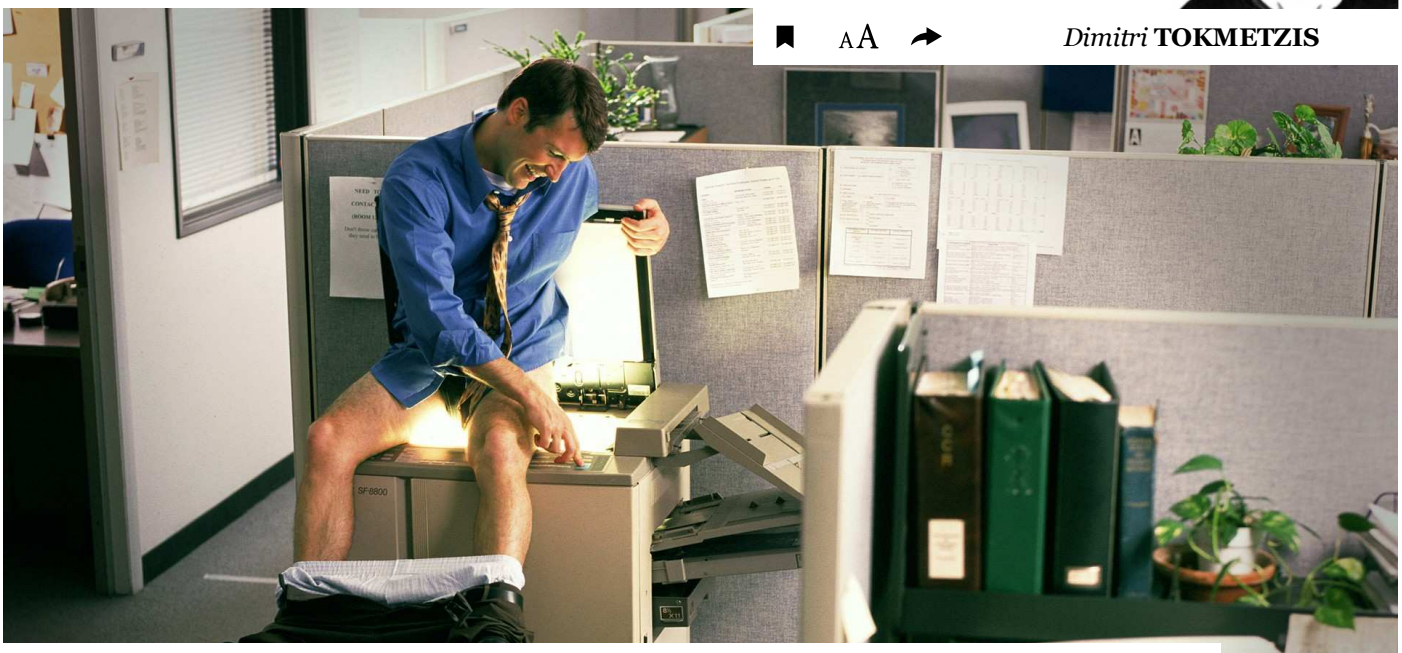

Foto: Joseph Hancock/Getty Images

Twee maanden geleden liet ik zien hoe duizenden mensen zeer privacygevoelige informatie prijsgaven door gebruik te maken van een downloadprogramma. Een beveiligingsonderzoeker was erin geslaagd om een beveiligingsfout te misbruiken om honderden haarscherpe paspoortscans, belastingaangiften, DigiD's en andere gevoelige documenten te bemachtigen.

Je hoeft geen programmeur te zijn om aan dit soort documenten te komen. Een oplettende lezer, Harmen Jeurink, ontdekte dat in copyshops dit soort documenten ook voor het

Lees hier: Zo raa duizenden mense downloaden hun kwijt.

grijpen liggen. Gastcorrespondent Maaike Goslinga ging gewapend met een usb-stick op pad en ontdekte dat wijzelf de grootste vijanden van onze privacy zijn.

hun paspoort kw downloaden.

Een hond met een luier om: het is een grappig en onschuldig beeld. Veel minder onschuldig zijn de andere documenten die op de computers van diverse onderzochte copyshops in Amsterdam, Rotterdam en Groningen te vinden zijn. Met één muisklik heb ik toegang tot bankafschriften, paspoortkopieën, loonstroken, vliegtickets, arbeidscontracten en een hele rits cv's. De copyshop blijkt een goudmijn van fraudegevoelige informatie te zijn die, eenmaal in foute handen, misbruikt kan worden voor identiteitsfraude. Maar wie is hier de schuldige van het beveiligingslek: de printwinkel of toch de klant?

Een erfenis van 40.000 euro

Zacht neurie ik mee met de tekst die voor de afstudeerborrel van Juul is geschreven — een tekst die, zo leest het document dat ik aanklik, gezongen moet worden op de klanken van Jody Bernals '*Que si que no*.' Juul hoeft zich eigenlijk niet druk te maken. De andere documenten die ik bij alle bezochte copyshops aantref zijn namelijk veel zorgwekkender. Het zijn bestanden op computers die klanten hebben gescand of hebben geüpload via een usb-stick of e-mail met het doel deze te printen.

Zo zie ik dat er op de bankrekening van een vrouw uit Groningen een tiental keer 415 euro is bijgeschreven. Ze is waarschijnlijk een huisbaas, want de omschrijvingen geven aan dat het om de maandelijkse huur gaat. Ook vind ik de loonstrook van een keukenhulp. Zijn maandloon is zo'n negen keer lager dan dat van de nieuwe marketingmanager van een groot internationaal concern, die volgens een contract dat ik op de desktop vind bijna 100.000 euro per jaar gaat verdienen.

En wat te denken van de brief van een Amsterdamse weduwe aan de Belastingdienst, waarin zij de op 40.000 euro getaxeerde erfenis van haar man noemt? Of de complete klassenlijst van een middelbareschoolklas, inclusief geboortedata en e-mailadressen? Binnen een klik leer ik wie er in de definitieve cast zit van een grote theaterproductie, dat Rebecca een kookcursus in Italië heeft gedaan en nu op zoek is naar een baan en dat een passagier een 'moslimmaaltijd' heeft besteld voor zijn vlucht naar Turkije.

Al deze documenten wekken dezelfde vraag op: hoe is het mogelijk dat ik een copyshop kan inlopen en toegang heb tot deze bijzonder gevoelige informatie, die door criminelen gebruikt kan worden voor identiteitsfraude, creditcardfraude of oplichterij? De copyshop laat zien dat de moderne dief de post niet meer uit je brievenbus hoeft te vissen en geen getrainde hacker hoeft te zijn. Hij is simpelweg uitgerust met een usb-stick.

Openbare computers blijven onveilige dingen

Natuurlijk is de copyshop deels debet aan dit beveiligingslek. Dat geüploade of gescande

documenten zo makkelijk door anderen kunnen worden ingezien is een grove fout. Zeker omdat Nederlanders steeds meer online met dienstverleners moeten communiceren en dus een schat aan digitale vertrouwelijke data hebben.

Gezegd moet worden dat de meeste copyshops met een carrouselsysteem werken, wat betekent dat elke computer aan het eind van de dag naar de fabrieksinstellingen wordt teruggezet. Dit geldt voor de meeste plekken met openbare computers, zoals bibliotheken, scholen, vliegvelden en internetcafés. Toch zijn er nog plekken – zo blijkt na een rondvraag – waar alles eens in de zoveel tijd handmatig wordt verwijderd. Zo kunnen documenten blijven rondzwerven en eventueel in foute handen terechtkomen.

Makkelijk is het wel, om met een beschuldigend vingertje naar de copyshop te wijzen. Mag deze openbaarheid van gegevens überhaupt een lek worden genoemd? Het is toch voornamelijk de gebruiker zelf die hier in de fout gaat. Bestanden worden argeloos geüpload of gescand naar een openbare computer, om vervolgens nooit meer te worden verwijderd. Want waarom zou je? Niemand klikt ooit op die oninteressante T-Mobile-facturen en uittreksels van de Kamer van Koophandel, toch?

Digitaal bewustzijn begint bij jezelf

Met zo'n duizend klanten per week weet André Pater van Printerette in Amsterdam als geen ander hoe mensen omspringen met hun persoonlijke gegevens. Elke dag verwijdert hij weer nieuwe bestanden van zijn computers, meldt hij nog ingelogde e-mailaccounts af en vult hij de bak met vergeten usb-sticks aan. 'Er is bijna niet tegen op te boksen. Wij gaan er wel achteraan, maar uiteindelijk vergeten mensen dat het verwijderen van bestanden vooral hun eigen verantwoordelijkheid is en niet alleen die van ons.'

Ik bel met een vrouw uit Amsterdam. Van haar heb ik in een copycenter een telefoonfactuur gevonden, waarop precies staat met wie ze heeft gebeld en hoe lang. Eén mobiel nummer springt eruit. Het blijkt het nummer van haar man te zijn, die mij later bezorgd belt met wat vragen. Ik vertel het stel dat ik hun adresgegevens, rekening- en telefoonnummer makkelijk kon achterhalen. Nou ja, achterhalen: de factuur stond open en bloot op een desktop, klaar om uitgeprint, gedownload of gekopieerd te worden.

De man, die de factuur voor zijn vrouw via een online account had gedownload en uitgeprint, was zich van geen kwaad bewust. Hij ging ervan uit dat de winkel zijn bestand wel zou wissen. Wel gaf hij toe dat hij veel documenten van anderen was tegengekomen op de desktop van de computer. Maar kon dat kwaad?

Wis je sporen op een openbare computer

Zoals Dimitri Tokmetzis eerder schreef, zijn deze gegevens allesbehalve onschuldig. Met een rekeningnummer en adres kan iemand heel makkelijk spullen op rekening kopen en

deze op een ander adres laten bezorgen. Het afsluiten van een telefoonabonnement gaat al met een simpele paspoortkopie. Gestolen gegevens kunnen ook makkelijk worden gebruikt om een lening te laten afsluiten en bankpasjes aan te vragen. En als het leed is geschied, is het buitengewoon moeilijk een schuldige aan te wijzen.

Identiteitsfraude wordt door digitalisering steeds makkelijker. Criminelen kunnen op slinkse wijze bankrekeningnummers, wachtwoorden en andere gevoelige gegevens ontfutselen door mensen naar valse websites te lokken (het zogeheten phishing) of te hacken, of door computers te infecteren met malware. Maar een rondje copyshops vertelt een nieuw verhaal: digitale lekken veroorzaken wij dus ook zelf. Uit gemakszucht, luiheid of onwetendheid.

Als je een openbare of gedeelde computer gebruikt, zorg dan dat je je sporen wist om je privacy te beschermen. Of het nu om inloggegevens of vertrouwelijke documenten gaat: verwijder je surf- en downloadgeschiedenis en je documenten en leeg de prullenmand. En, een lesje van de copyshop: behandel je usb-stick alsof het je smartphone is. Die laat je immers ook niet zonder vergrendeling op de winkelbalie liggen.

Deze explainer is geschreven door gastcorrespondent Maaike Goslinga.De onderzochte copyshops zijn inmiddels op de hoogte gebracht van deze kwestie. De Correspondent bedankt tipgever Harmen Jeurink voor zijn oplettendheid en verhaal.

Zo raakten duizenden mensen tijdens het downloaden hun paspoort kwijt

Populaire downloadnetwerken als eMule zorgen ervoor dat zeer gevoelige informatie - vaak ongemerkt - van je computer op het internet belandt. Duizenden paspoortscans, belastingaangiften en financiële administraties kunnen zo eenvoudig worden gebruikt worden om fraude mee te plegen. Het lek toont wat er kan gebeuren als techniek de scheidslijn tussen privé en openbaar doet verdwijnen.

Lees verder

Hoe beveilig je documenten op je computer?

Door allerlei beveiligingslekken kun je per ongeluk persoonlijke documenten online zetten. Hoe kun je dit voorkomen? Drie tips.

Lees verder