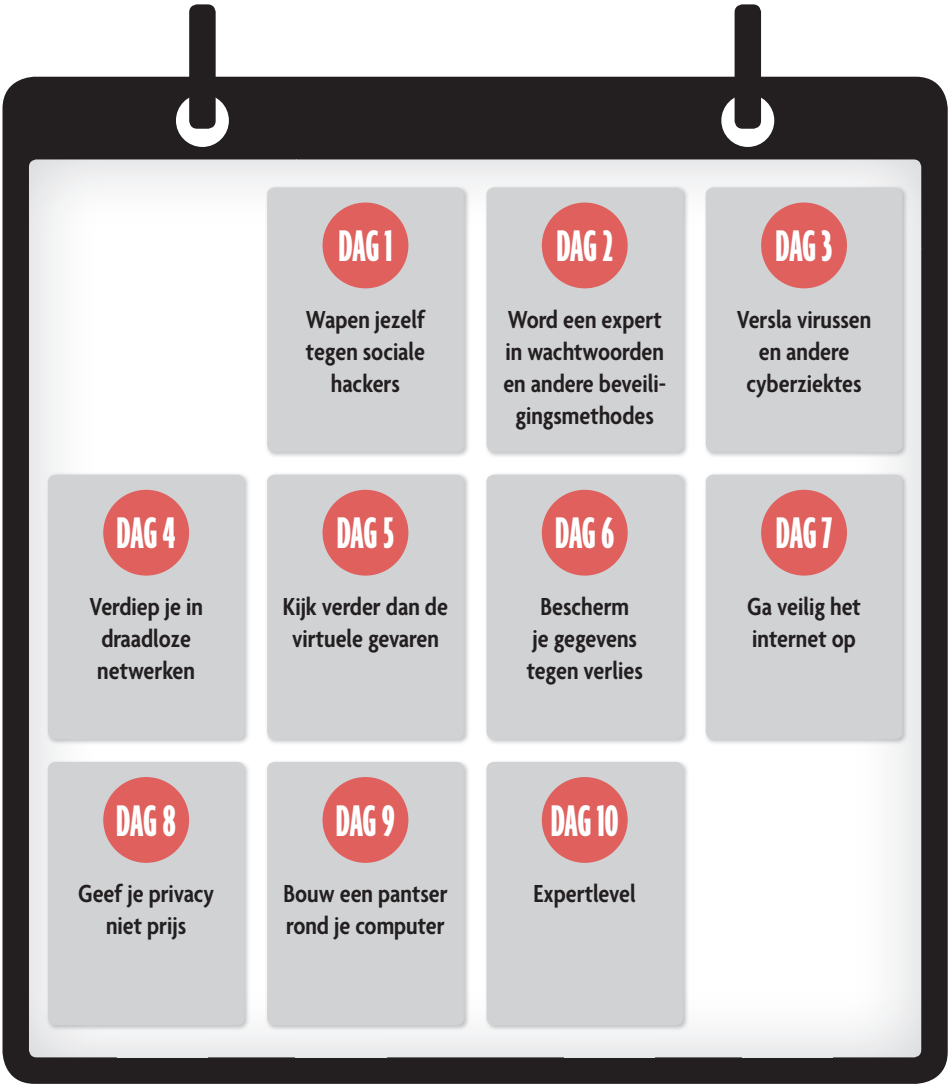
CYBER VEILIG IN 10 DAGEN



D/2019/45/434 – ISBN 978 94 014 6365 2 – NUR 740, 980

Vormgeving omslag: Bjorn D'Hulst
Vormgeving binnenwerk: Wendy De Haes

Uitgeverij LannooCampus maakt deel uit van Lannoo Uitgeverij,
de boeken- en multimediadivisie van Uitgeverij Lannoo nv.

Uitgeverij LannooCampus
Vaartkom 41 bus 01.02
3000 Leuven
België
www.lannoocampus.be

Postbus 23202
1100 DS Amsterdam
Nederland
www.lannoocampus.nl

INHOUD

INLEIDING

2244 keer per dag of elke 39 seconden. Zo vaak ligt ergens een computer, die aan het internet gekoppeld is, onder vuur door hackers. Dat blijkt uit een studie van de Universiteit van Maryland. Het was één van de eerste studies (2007) die concreet het aantal aanvallen testte. Vaak geven ze daarbij een kleine speldenprik, om te kijken hoe gemakkelijk het is om virtueel in te breken. Toch is het aantal schokkend veel.

Als je dat weet, wil je natuurlijk op zoek gaan naar manieren om je te beschermen. Wees daarbij altijd voorzichtig. Door op een link te klikken, van een website die je schijnbaar wil helpen, installeer je mogelijk een valse virusscanner op je computer, die net je gegevens steelt en doorsluist. Soms bots je ook op moeilijke teksten, waarmee mensen je wel willen verder helpen, maar waaraan vooral techneuten wat hebben. Dat wil dit boek anders doen.

Het informeert je over de basisbegrippen van cyberveiligheid. Het is geen saaie cursus, maar een snelle, duidelijke en interessante introductie die ervoor zorgt dat je het laatste nieuws over cyberveiligheid begrijpt zonder alle details te kennen.

Je spijkert je basiskennis bij, maar gaat ook verder dan dat. Je krijgt een antwoord op de waarom-vraag. Waarom moet je een lang wachtwoord verzinnen, in plaats van een kort? En wat is er nu erg aan klikken op een phishinglink?

Andere boeken zijn te omslachtig of geven te weinig praktische tips. Ze gaan te diep of net niet diep genoeg. Je achtergrondkennis moet in

veel gevallen ook reeds zeer goed zijn, of je riskeert het boek al snel aan de kant te leggen. Door tien dagen lang telkens één hoofdstuk uit deze publicatie te lezen, leer je snel bij op een eenvoudige manier.

Elke dag zul je iets nieuws te weten komen en keuzes moeten maken, als je dit boek doorneemt. Daarbij is het zoeken naar een balans tussen veilig en handig. Hoe veiliger je iets maakt, des te moeilijker het gebruik ervan wordt. En wil je het handiger, dan wordt het doorgaans minder veilig. Zo is het gebruik van eenzelfde wachtwoord op al je accounts vanzelfsprekend handig, maar helemaal niet veilig. Zoek voor jezelf het juiste evenwicht.

Wil je jezelf of je hele gezin wapenen tegen cybercriminelen? Dit boek helpt je daarbij in tien dagen.

DAG 1

WAPEN JEZELF TEGEN SOCIALE HACKERS

De allereerste truc waarmee kwaadwillige *scriptkiddies* en hackers je proberen te misleiden, heeft weinig met technologie te maken, maar vooral met psychologie. De menselijke psyche is ingewikkeld. Wetenschappers hebben ons brein nog altijd niet helemaal doorgrond, maar wie enkele basisprincipes kent, kan heel makkelijk anderen misleiden.

Ook hackers weten dat. Ze proberen met de kracht van die kennis anderen op te lichten. Ze pogen je zo ver te krijgen dat je zelf informatie geeft, zonder dat ze daarvoor moeten inbreken in computers. Die techniek heet *social engineering*.

Social engineering is de kunst van het misleiden van, onder andere, computergebruikers. Maar eigenlijk ook iedere vorm van misleiding van mensen om gegevens te ontfutselen of om te kunnen frauderen.

De Amerikaan Kevin Mitnick beheerst deze techniek perfect. Hij was ooit een van de meest gezochte hackers in de Verenigde Staten en is meester in het misbruiken van het brein van anderen. Mitnick begon aan zijn carrière toen hij twaalf jaar oud was. Hij zocht toen een manier om gratis met de bus te rijden. Mitnick maakte een buschauffeur wijs dat hij een toestel nodig had om buskaartjes te knippen, voor een schoolproject. Via de man kwam Mitnick te weten waar hij zo een knipper kon kopen. Het ging in dit geval om een exemplaar dat gebruikt werd om in de buskaartjes een gaatje te knippen, waardoor die nog geldig zouden zijn voor een overstap. Vervolgens ging Mitnick in containers op zoek naar weggegooide kaartjes. Die knipte hij zelf, om van de ene op de andere bus over te stappen. Zo kon hij zijn zakgeld aan andere zaken dan transport besteden.

In de jaren die volgden legde Mitnick zich helemaal toe op het misleiden van anderen. Zo lichtte hij werknemers van telefoniebedrijven op, zodat hij gratis internationaal kon bellen. Mitnick werd in 1995 opgepakt en schreef nadien het boek *The art of deception*, waarin hij manieren van social engineering en het waarom daarvan uit de doeken doet.

NOG ELKE DAG EEN PROBLEEM

Vandaag is iedereen er zich van bewust dat oplichters bestaan. Je zou vermoeden dat bijvoorbeeld medewerkers van telefoniebedrijven niet meer te misleiden vallen, omdat iedereen van Mitnick geleerd heeft of minstens al eens een fraudeur aan het werk zag in een film? Wel, ook nu zijn er helaas nog genoeg voorbeelden van social engineering.

Zo zijn er callcenters, vaak in India, zo blijkt uit een onderzoek van de Amerikaanse Federal Trade Commission (2012, *FTC Halts Massive Tech Support Scams*), waarvan medewerkers doen alsof ze werken bij onder andere de technologiebedrijven Microsoft, Dell of McAfee. Ze vragen je enkele handelingen uit te voeren op je computer, omdat die zogezegd een 'virus' zou bevatten. De beller wil je probleem verhelpen door je een website te laten bezoeken. Maar eigenlijk stuurt de hacker je naar een site waarop malware staat of vraagt hij je om software te installeren waarmee hij je computer wil overnemen. Daarom is het belangrijk om nooit op dergelijke telefoontjes in te gaan of onmiddellijk in te haken.

Nog een veelgebruikte methode is dat iemand zich voordoet als een helpdeskmedewerker en vraagt om je wachtwoord en gebruikersnaam door te geven, ter verificatie. Uiteraard is dat nooit een goed idee, maar toch gebeurt het nog elke dag.

Maar zelfs de trucs van Mitnick worden nog altijd volop gebruikt. Er is een reden waarom bedrijven gevoelige documenten versnipperen voor ze die in een container dumpen. Het zou voor iemand met slechte bedoelingen simpel zijn om daar even in te duiken en zo wachtwoorden, betalingsgegevens of namen van werknemers te stelen. Die techniek is zo oud als de straat en heet bij hackers dumpsterdiving.

Toch zijn er hackers die niet eens zo ver moeten gaan. Ze gebruiken de eenvoudige techniek van shouldersurfing. Ze kijken gewoon even mee als we met onze toestellen werken. We staan er vaak niet bij stil, maar we typen geregeld achteloos ons wachtwoord in, bijvoorbeeld terwijl we bij de bakker aanschuiven. Of we zitten met onze laptop op een ter-

ras te schrijven aan een e-mail naar onze werkgever en we hebben niet in de gaten dat achter ons iemand meeleest.

Het lijkt wat vergezocht, maar shouldersurfing is misschien wel de meest gebruikte vorm van informatievergaring. In sommige gevallen kan dit echt een bedreiging vormen. Zo zal een dief graag eerst de pincode of toegangscode van je smartphone kennen, voor hij je toestel steelt. Of hij zal over je schouder meekijken om te memoriseren welke apps je gebruikt of wat de naam van je partner is. Of hij zal je afluisteren terwijl je aan de telefoon bent, om zo veel mogelijk details te weten te komen. Al die gegevens kunnen achteraf nuttig zijn om je op te lichten, door die informatie te misbruiken.

GERICHT INFORMATIE MISBRUIKEN

Allemaal goed en wel, maar daar trap je niet in, toch? Wel, als iemand jou écht als doelwit uitkiest, dan ben je kwetsbaarder dan je denkt. Je hoeft niet heel ver te zoeken naar personen die graag social engineering toepassen. Zo hebben je kinderen er mogelijk alle baat bij om zo veel mogelijk wachtwoorden te verzamelen. Ook dat van je Amazon-account kan handig zijn. Net zoals de wachtwoorden van je domotica, om de logbestanden te wissen, zodat je als ouder niet meer kunt te weten komen wanneer ze het huis zijn binnengeslopen na een avondje stappen. Ze kunnen meekijken in je agenda, om te weten wanneer jullie het huis uit zijn, of ze proberen misschien wel je e-mails mee te lezen. Er groeit momenteel een generatie op die wel degelijk slim genoeg is om dat allemaal te doen.

Het verzamelen van informatie op zich is natuurlijk nog geen social engineering. Het misbruiken daarvan wél. Stel, je krijgt iemand aan de deur die enkele weken eerder jouw waterrekening uit het vuilnis gevist heeft. Hij kent niet alleen jouw adres, maar ook je klantnummer en kan dat moeiteloos aflezen van een document. Op dat moment is de kans groot dat je de oplichter gelooft, want hij beschikt over cruciale informatie die alleen de watermaatschappij kan bezitten.

Misschien nog het belangrijkste misdrijf dat hackers kunnen plegen, is identiteitsfraude. Met voldoende informatie kunnen ze zich tegenover jou als iemand anders voordoen, of doen alsof ze jou zijn tegenover mensen die je kent! Aangezien de meeste mensen heel veel communiceren via berichten en e-mail, is het niet eens zo moeilijk om 'te doen alsof'.

TIP

Social engineering is een fascinerend maar erg uitgebreid thema. De basis is dan wel eenvoudig, maar het is een veelzijdige vorm van oplichting. In realiteit zijn er tientallen soorten aanvallen die criminelen hanteren.

Op de website Reddit is het subforum over social engineering fascinerende lectuur. Daar melden slachtoffers en daders vaak nieuwe technieken. Je vindt het op https://www.reddit.com/r/SocialEngineering (Engels).

Een vorm van gerichte social engineering bedreigt vooral grote bedrijven. Hackers proberen daarbij eerst zo veel mogelijk te weten te komen over de CEO, de baas van de onderneming. Daarna doen ze alsof ze hem/haar zijn en vragen ze aan een medewerker via e-mail of zelfs per telefoon om een miljoen over te schrijven naar een rekening ergens in het buitenland.

De praktijk lijkt recht uit een film te komen, maar jaarlijks zijn er verschillende gelijkaardige gevallen. Ook bij grote banken gebeurde het al. De hackers zijn vaak erg overtuigend en wissen hun sporen meestal zeer goed uit, zodat ze achteraf nagenoeg onvindbaar zijn.

Uit voorgaande voorbeelden blijkt alleszins dat een beetje *'security awareness'*, zeg maar een zekere bewustwording over deze technieken, niet alleen voor personeel van bedrijven belangrijk is, maar ook voor gezinnen. Over informatiebescherming zou binnen een familie eigenlijk gepraat moeten worden. Iedereen zou een gezonde achterdocht moeten koesteren voor wie de familie belt, e-mailt, berichten en brie-

ven stuurt en zelfs tegenover wie voor de deur staat. In dit geval geldt eigenlijk: een beetje paranoïde zijn is best oké.

Omdat we tegenwoordig allemaal een groot deel van ons leven online doorbrengen, lekken we veel informatie zonder dat te beseffen. Oude blogposts, filmpjes en foto's die je vrienden op het internet zetten of zelfs het personeelsmagazine zijn daar voorbeelden van. Je kunt veel van die informatie terugvinden via zoekmachines als Google.

Maar er zijn ook onderzoekers gespecialiseerd in het naar boven spitten van info die er op het eerste gezicht niet is: door verbanden te leggen of door bronnen te doorzoeken die niet gemakkelijk te vinden zijn, tenzij je weet waar je moet zoeken. Dergelijke onderzoekstechnieken worden ook gebruikt door onze politie, om potentiële daders op te sporen, door journalisten, om verhalen te vinden, en zelfs door werkgevers, voor ze iemand aannemen. Het heet openbronnenonderzoek of Open-Source Intelligence (OSINT): het doorzoeken van bronnen die publiek zijn.

De laatste jaren zijn openbronnenonderzoekers echte specialisten geworden in hun vakgebied. Nieuwssites zoals https://www.bellingcat.com hebben er zich in gespecialiseerd, en programmeurs bieden diensten aan waarmee zo een onderzoek makkelijker te voeren valt.

Wil je zelf openbronnenonderzoek doen, probeer dan Maltego van Paterva uit. De laatste versie download je op https://www.paterva.com. Met dit technisch erg geavanceerde programma bouw je een schema op om de informatie die je vergaart eenvoudig weer te geven en automatiseer je heel wat zoekacties.

PHISHING

Ook phishing is een vorm van social engineering die heel specifiek jou als slachtoffer kan uitkiezen. Criminelen sturen je e-mails die erg lijken op die van een echt bedrijf en hopen dat je op de malafide links erin klikt.

Phishing is misschien wel de meest gebruikte manier om gebruikers op het internet te misleiden. De e-mails zijn gemaakt om te lijken op die van iemand (of iets) die je kent, bijvoorbeeld je bankbediende of je supermarkt. Het doel is steeds om je naar een andere website te lokken, je (kredietkaart)gegevens te stelen of je op te lichten op nog andere manieren. Ze bevatten soms ook een link naar malware of hebben een bijlage waarvan de criminelen hopen dat je die opent. Je computer raakt dan geïnfecteerd. Nochtans zijn deze mails doorgaans wel goed als vals te herkennen.

Vandaar deze checklist:

» **Ken je de persoon?**
Vraag je eerst af of je wel een e-mail van deze persoon of instantie verwacht. Zo kun je de meeste problemen al vermijden. Een bank die je niet kent of waar je geen rekening opende? Een persoon waarvan je nog nooit gehoord hebt? Dan moet je toch al twee keer nadenken.

Je ontvangt bijvoorbeeld een e-mail over een pakje dat onderweg is, terwijl je helemaal geen weet hebt van een bestelling. Let dan op, dit kan een oplichter zijn. Wil je zeker zijn? Bel dan even met de webwinkel of stuur die zélf een e-mail vanaf zijn website (via de helpdesk). Je kunt de afzender ook aanspreken via sociale media.

Hetzelfde geldt voor e-mails van banken: Is het een bank die je niet kent? Niet op ingaan. Is het wel je eigen bank? Bel even naar je kantoor als de e-mail verdacht lijkt.

» **Is de mail afkomstig van een professioneel e-mailadres?**
Je zult nooit een e-mail van je bank of belastingdienst ontvangen via een dienst zoals Gmail of Outlook.com. Zij zullen altijd het mailadres gebruiken van hun bedrijf: bijvoorbeeld eindigend op 'bnpparibasfortis.be'. De kans dat een officiële instantie je probeert te bereiken met een 'gratis' e-maildienst is zo goed als onbestaand.

Weet wel: hackers kunnen een e-mailadres ook nabootsen. Het is dus niet altijd omdat je mails van een professioneel adres ontvangt, dat die ook veilig zijn. Gebruik daarom nog altijd je gezond verstand. Het controleren van een e-mailadres is maar een van de manieren om phishingmails te herkennen.

» **Bekijk de aanspreking.**
Hoe word je in een e-mail aangesproken? Komt dat overeen met vorige berichten? Als een advocaat je altijd aanspreekt met 'Geachte heer X', zal hij dat niet plots anders doen bij een volgend bericht. Bovendien zal een phishingmail in heel wat gevallen niet gepersonaliseerd zijn en beginnen met 'Beste klant' of 'Geachte klant van bank X'. Ook dan moet je dus voorzichtig zijn.

» **Controleer het taalgebruik.**
Hoewel phishingmails tegenwoordig vaak in relatief goed Nederlands geschreven zijn, gebeurt het toch nog geregeld dat criminelen niet de moeite nemen om foutloos te schrijven. Ze vertalen een Engelstalige e-mail met een goedkope vertaaldienst of ze spreken maar een beetje Nederlands en maken fouten tegen de basisspelling.

» **Wat vragen ze en is het logisch om dat per e-mail te doen?**
Een professioneel bedrijf zal je nooit via e-mail vragen naar een wachtwoord en gebruikersnaam of naar bankgegevens. Deze informatie e-mailen is namelijk niet veilig. Ook een kopie van je identiteitskaart doorsturen is uit den boze. Vraagt iemand dat wel? Dan is de kans groot dat het om criminelen gaat. Je bank zal je ook niet in een e-mail vragen om grote stortingen te doen. Krijg je wel deze vraag via een e-mail, dan bel je maar beter even om de gegevens daaruit te controleren. Het gebeurt dat criminelen net op het

juiste moment een e-mail sturen die echt lijkt te zijn. Bijvoorbeeld wanneer ze jouw mailbox in de gaten houden en jij op een bepaald moment met de notaris e-mailt over de aankoop van een huis. Bel in een dergelijk geval altijd even om onder meer het rekeningnummer telefonisch te checken. Telefoneer trouwens nooit zomaar het nummer dat in de e-mail staat, maar zoek het even op via Google, in een onlinetelefoonboek, in de contacten op je smartphone of op een officieel document.

» **Naar waar linkt de e-mail door?**
Bevat de e-mail een hyperlink, check dan of die naar de correcte website verwijst. Dat kun je meestal makkelijk controleren door je muisaanwijzer over de hyperlink te houden. In veel gevallen komt dan naast je muispijltje het volledige adres te staan. Lees je daarin bijvoorbeeld goOgle.gl.com of argenta.co.ru? Dan gaat het om een phishingmail. Ben je niet zeker? Open dan je browser en typ zelf de correcte URL in, in plaats van op de link in de e-mail te klikken. Die kun je vinden op officiële documenten zoals een factuur en staat (meestal) ook bovenaan Google als je er naar zoekt.

Hackers staan niet stil en zoeken steeds naar nieuwe manieren om mensen op te lichten. Zo zijn er inmiddels al variaties op phishing, namelijk smishing en *vishing*. Smishing staat voor sms-phishing. Daarbij sturen oplichters sms'jes naar potentiële slachtoffers, om persoonlijke informatie te weten te komen.

Vishing komt van voice-phishing. Via een telefoongesprek proberen de hackers gevoelige info bij je te ontfutselen of je te overhalen om grote bedragen naar hen over te schrijven, net zoals de callcenters uit India dat proberen.

CHECKLIST DAG 1

Op Dag 1 beveiligen we niet onze toestellen, maar wel onszelf:

- **Geef niet zomaar persoonlijke informatie aan anderen door (zoals wachtwoorden).**
- **Gooi geen documenten in het huisvuil waaruit je identiteitsgegevens af te leiden vallen.**
- **Versnipper gevoelige documenten voor je ze weggooit.**
- **Twijfel altijd aan iedereen die je opbelt en probeer te achterhalen wie je écht aan de lijn hebt. Desnoods door het telefoonnummer op te zoeken in Google.**
- **Ontvang je belangrijke berichten of e-mails? Bel dan eerst even met de persoon die deze naar jou gestuurd heeft. Gebruik daarbij altijd het telefoonnummer dat in jouw smartphone staat en niet het nummer dat in de e-mail vermeld wordt.**
- **Vertrouw je iemand niet, dan kun je altijd naar zijn of haar bedrijf bellen, om na te gaan of deze persoon daar wel werkt én een afspraak met jou heeft.**
- **Bescherm jouw informatie zo goed mogelijk, want hoe meer iemand over je weet, des te makkelijker hij of zij jou kan misleiden.**