Nico Joos & Katrien Van Effelterre

STOP PHISHING

30 tips om je online veiligheid te verhogen

MANTEAU

Inhoud

HOE HET ALLEMAAL BEGON

Geboren worden is niet iets waar je voor kiest. Laat staan dat je kan kiezen in welk tijdperk of op welke plek het gebeurt. Zelf ben ik een kind van een septembermaand uit de late jaren zeventig. Leg je mijn tijdslijn naast die van het internet, dan stel je vast dat ik volwassen werd toen het internet nog een kleuter was. Technisch gezien bestond er al veel eerder iets wat uiteindelijk zou uitgroeien tot het internet zoals we het vandaag kennen. Maar de meesten onder ons waren pas aan het einde van de jaren negentig getuige van de intrede van sciencefictionachtige modems die buitenaardse geluiden voortbrachten, terwijl de onzichtbare poorten van de online wereld knarsend openschoven. Wat in die tijd – hoe vervelend toch – steevast gepaard ging met een bezette telefoonlijn. Alsof het gisteren was herinner ik me nog de discussies met mijn ouders over dat ongemak. Om nog maar te zwijgen over het moment waarop de telefoonrekening in de analoge brievenbus viel! Dat waren beslist niet de gezelligste momenten ten huize Joos. Gelukkig werd niet veel later op veel adressen de huisvrede hersteld door de intrede van het bekabelde internet. Dat was het verlossende begin van de situatie die we vandaag nog steeds kennen. We betalen een

vaste prijs aan een internetprovider en krijgen daarvoor een internetverbinding die veelal performant genoeg is om ons naar hartenlust te laten surfen.

Ooit was het anders. Het internet is ontstaan uit de verbinding van computernetwerken. Die computernetwerken zijn op hun beurt ontstaan door – je raadt het al – het verbinden van computers.

Voordat we internet hadden, moesten we onze computerbestanden op een fysieke drager opslaan. Dat kon op de computer zelf of op een diskette, later op een cd-rom, of nog later op een USB-stick. Telkens ging het om een drager die we in de computer moesten plaatsen om iets te kunnen opslaan. Vroeger was dat vrijwel de enige manier om gegevens uit te wisselen tussen mensen en computers. Iemand had iets op een diskette geplaatst, gaf die diskette door aan iemand anders en die andere persoon kon ermee verder. Dat gebeurt vandaag nog, bijvoorbeeld via USB-sticks.

In die context was misbruik van je gegevens alleen mogelijk als iemand zich toegang wist te verschaffen tot je computer, of tot zo'n diskette waarop je computerbestanden met gevoelige informatie had opgeslagen. De toegang tot die gegevens was een zichtbaar proces waarvan mensen zich erg bewust waren. Zo moest iemand met slechte bedoelingen al fysiek in je huis aanwezig zijn om zijn slag te kunnen slaan. Bovendien moest hij de weg vinden naar de kamer waar dé computer stond – er was er immers hoogstens één per gezin – en dan ook nog toegang tot die computer krijgen.

Diskettes, die meestal een memorabele opslagcapaciteit van 1,44 megabyte hadden, werden vaak bewaard in een doosje, een lade, een kast of een aktetas. Om dat soort dingen kwijt te raken, moest je dus al fysiek bestolen worden, of je tas per ongeluk vergeten in de trein. En zo populair waren diskettes bij

dieven helemaal niet, want mensen hadden niet de gewoonte om hun meest gevoelige informatie op zo'n ding op te slaan. Logisch, want diskettes gingen ook makkelijk stuk, dus erg betrouwbaar waren ze niet.

Vandaag echter vertrouwen we zowat al onze gegevens toe aan een computer en is het eerder uitzonderlijk om dat niet te doen. Wie bezit vandaag nog een boekje met daarin de namen en telefoonnummers van vrienden en familieleden? Wie gebruikt er nog een papieren agenda? Wij alvast wel, maar niet zonder het besef dat we daarmee uitzonderingen zijn.

Hét internet

Zodra we computers met elkaar begonnen te verbinden, konden we spreken van een netwerk. Dat gebeurde eerst nog binnen één gebouw, vaak binnen één kamer. Maar in ieder geval bestond er al gegevensuitwisseling tussen computers onderling, zonder dat iemand met een diskette van de ene computer naar de andere moest lopen.

Door het gebruik van ondergrondse kabelinfrastructuur ging men later computers en computernetwerken met elkaar verbinden over de grenzen van gebouwen, landen en hele werelddelen heen. *Et voilà*, mogen we je voorstellen: het internet.

We spreken altijd over hét internet. Er is er maar één. Zoals dé aarde. Net zoals de aarde is het internet een plek voor ons allemaal, dus moeten we afspraken maken over de manier waarop we die plek gebruiken. Die afspraken zijn er geleidelijk gekomen, waardoor we vandaag bijvoorbeeld e-mails naar elkaar kunnen sturen, websites kunnen bezoeken en apps kunnen gebruiken. Voor al die toepassingen werden technische afspraken gemaakt, en wie zich aan die afspraken houdt, slaagt erin om ergens bij iemand een stukje informatie op een scherm te toveren. Niets minder dan een wonder.

Een wonder dat nog helemaal niet zo oud is. Mijn zoon zal het vast tegenspreken, maar zelf beschouw ik de man in de spiegel nog niet als een oud exemplaar van het menselijk ras. In het jaar 2000 behaalde ik mijn diploma en begon ik te werken. Mijn ouders vertelden trots aan iedereen die het wilde horen dat hun zoon 'voor computer' had geleerd. Internet via een kabelverbinding stond in België in die tijd nog in zijn kinderschoenen. Pas tijdens de afgelopen twintig jaar zijn we geëvolueerd van een situatie waarbij we af en toe een mailtje naar elkaar stuurden en louter informatieve websites bezochten, naar een leven waaruit internettoepassingen niet meer weg te denken zijn. Apps, smartphones, webbanking en sociale media zijn even vanzelfsprekend geworden als de bomen in een bos. Ook is de gebruiksvriendelijkheid van al die toepassingen enorm geëvolueerd. Toen ik 'voor computer' leerde, beschouwde iedereen me als een van die uitzonderlijke nerds die in staat waren een computer aan de praat te krijgen, en dan ook nog de durf hadden om ermee aan de slag te gaan. Want mensen waren bang voor computers, zelfs voor de exemplaren die in hun eigen huiskamers stonden. Ze moesten worden opgeleid om te werken met één specifiek programma. Vaak werd hun computer simpelweg vereenzelvigd met dat ene programma dat ze hadden bestudeerd en dat ze gebruikten om bijvoorbeeld teksten te schrijven. Om daar goed in te slagen moesten ze allerlei toetsencombinaties uit het hoofd leren, bijna zoals de Latijnse woordjes op school.

Vroeger loonde het dan ook niet de moeite om mensen via computers op te lichten. Slechts weinigen konden echt goed met het ding overweg, en nog minder werd het gebruikt om gevoelige data mee uit te wisselen. Vandaag leven we in een totaal andere realiteit, en is de digitale wereld voor criminelen een eindeloos walhalla van instant bereikbare opportuniteiten.

Een kind kan de was doen

De grote softwarehuizen hebben ervoor gezorgd dat het gebruik van apps en sociale media zo simpel is dat mensen er zonder opleiding hun weg in vinden. Een kind kan de was doen. Enkele jaren geleden bestonden er nog geen 'specialisten in gebruiksgemak', vandaag zijn het uiterst gewilde IT-profielen. Dit zijn immers de mensen die uitzoeken waar jij en ik tegenaan lopen wanneer we software gebruiken. Ze worden ingehuurd door commerciële bedrijven die er alle belang bij hebben dat iedere burger een potentiële koper van hun product kan zijn. Door het commerciële belang wordt technologie sneller en gemakkelijker ingezet, wat enerzijds innovatie faciliteert en anderzijds de toegang tot digitale media democratiseert.

Stukje bij beetje hebben specialisten het gebruiksgemak opgevijzeld en de drempel naar de toegang tot de technologie verlaagd of weggenomen. Maar net het wegnemen van die drempel heeft tot een immens gevaar geleid. Mensen met minder goede bedoelingen gebruiken het internet als een gigantisch jachtterrein om anderen op te lichten. Ze laten geen kans onbenut om digitale gegevens waaruit munt te slaan valt, buit te maken. En die gegevens hebben we zelf ten overvloede ter beschikking gesteld. Zonder dat we het goed beseffen, springen we ongelooflijk slordig om met zoveel meer gegevens dan de luttele informatie die we vroeger aan onze goed verborgen diskettes toevertrouwden. Ooit waren we bang voor onze computer, hoewel er amper gegevens in waren opgeslagen. Nu vertrouwen we ons hele leven toe aan het internet, maar zijn we in die digitale speeltuin niet meer bang te maken. Logisch? Allesbehalve.

We worden allemaal meegezogen in een wereld die technologie inzet voor toepassingen die vroeger fysieke processen waren. Denk bijvoorbeeld aan je bankzaken. Hoe meer functies we van ons fysieke naar ons digitale leven verschuiven onder

het mom van gebruiksgemak, hoe interessanter het voor een crimineel wordt om van die digitale wereld zijn nieuwe jachtterrein te maken.

Cyberinbrekers

De meeste mensen verlaten nooit hun huis zonder de deur op slot te doen. Op de plek waar ons digitale leven zich afspeelt daarentegen, is het elke dag opendeur. Dieven kunnen dan ook op ieder uur van de dag of nacht, overal ter wereld, hun slag slaan. Vandaag is het voor een crimineel veel lucratiever om vanaf een afstand digitaal toegang te krijgen tot je bankrekening dan om in je huis in te breken en op zoek te gaan naar je portefeuille en juwelen. Geen wonder dus dat cybercriminaliteit zo actueel is geworden. Verhuizen wij onze waardevolle goederen naar de digitale wereld, dan verhuist de crimineel mee. Waren we vroeger alleen maar bezig met de beveiliging van ons fysieke huis, dan moet nu ook ons plekje in de digitale wereld van de nodige sloten en grendels worden voorzien. Nog maar weinig mensen laten hun dure fiets onbeheerd en zonder slot achter bij een winkel, om te verwachten dat die daar even later nog zal staan. Op dezelfde manier mag je ervan uitgaan dat een crimineel die je wachtwoord heeft weten te achterhalen, zal proberen je daarmee wat centen te ontfutselen. Dit kat-en-muisspel is in constante evolutie en de beveiligingsbehoeftes evolueren mee. Technieken worden uitgetest, gebruikers worden slimmer, maar de criminelen ook, waardoor er weer nieuwe technieken moeten worden ontwikkeld.

Deze hele evolutie in risico is uiteraard ook de bank- en verzekeringssector niet ontgaan. Bij veel banken kan je nu een speciale verzekering afsluiten die je beschermt tegen cybercriminaliteit. Maar zoals bij iedere verzekering is het belangrijk om de kleine lettertjes in de polis te lezen. Zo zal de schade

veroorzaakt door een woningbrand niet worden gedekt als die is ontstaan doordat je in de woonkamer een barbecue hebt aangestoken. Autoverzekeringen vermelden meestal dat je auto uitgerust moet zijn met een alarm van een bepaald type. In dezelfde lijn vereisen de verzekeringen tegen internetfraude dat gebruikers een basisbeveiliging toepassen, om hackers zo weinig mogelijk kansen te gunnen.

Net zoals je gewend bent het huis van je fysieke leven te beveiligen, kan je dat ook met je digitale leven doen. En dat hoeft helemaal niet moeilijk te zijn. Om inbrekers in je straat af te weren hoef je geen grachten rond je huis te graven, Mechelse herders te laten rondlopen in je tuin of een drie meter hoge prikkeldraad te plaatsen. Iedereen weet dat absolute veiligheid niet bestaat, maar dat het er vooral op neerkomt inbrekers met enkele eenvoudige ingrepen af te schrikken, waardoor ze al snel uitkijken naar een ander huis dat makkelijker te betreden valt. In de digitale wereld geldt precies hetzelfde. Honderd procent garantie heb je nooit. Maar enkele eenvoudige ingrepen kunnen er wel voor zorgen dat jij niet dat makkelijke doelwit bent.

Mensen hoeven niet bang te zijn voor het grote gevaar dat hacking heet. Vaak worden hackers afgebeeld als duistere figuren gekleed in een zwarte hoody waarvan de kap hun gezicht verbergt. Net zoals we aan het einde van de jaren negentig een beetje bang waren voor die computer met zijn rare geluidjes, zijn we dat nu ook voor die hackers. En als we nog niet bang zijn, dan worden we wel bang gemaakt. En toch kunnen we door middel van eenvoudige ingrepen die onzichtbare vijand wandelen sturen naar het volgende adres. Dat gaat zelfs vaak letterlijk op die manier. Net zoals woninginbrekers doen, komen hackers bij je langs om even aan de deur te voelen, te kijken of de ramen goed gesloten zijn en of er niet toevallig ergens een poortje openstaat. Wanneer ze binnen zijn geraakt, snuffelen ze rond om te zien of er iets waardevols te stelen valt. Als het

over je huis gaat, moet er dus wel degelijk iemand fysiek bij je langskomen. Dat schept al een zekere drempel. Maar in het geval van je computer en het internet gebeurt alles van een afstand. Hackers kunnen van de andere kant van de wereld in een fractie van een seconde langskomen op jouw digitale adres en uitzoeken of er een deurtje openstaat waarlangs ze kunnen binnenkomen. Het enige wat zo'n hacker nodig heeft, is een computer, een internetverbinding en kennis. Dat laatste is een gewild goed. Heel dikwijls zijn hackers ongelooflijk bedreven netwerkspecialisten en is het zonde dat ze die kennis niet ten dienste van bedrijven of overheden inzetten.

Omdat men dus, zonder gezien te worden, even aan je deurklink kan komen morrelen, zorg je er maar beter voor dat je deur goed vergrendeld is. Een veiligheidsslot kan al veel helpen. Maar wees dan ook niet slordig met de sleutel. Want wat heb je aan een peperduur, onverwoestbaar slot als de sleutel onder de deurmat ligt? Het klinkt absurd, maar het is op veel plekken de digitale realiteit.

Mensen zijn vooral kwetsbaar op terreinen die ze niet goed kennen. Velen raken dan ook makkelijk onder de indruk van het jargon dat vermeende specialisten gebruiken om hun slachtoffer in de val te lokken. Hoe minder je er zelf van kent, hoe makkelijker je je kritische zin laat varen en in de val trapt. Zo gebeurt het dat hackers erin slagen om gegevens te bemachtigen waarmee ze hun slachtoffers kunnen bestelen. Zo gek is dat niet, want heel ver hoeven we niet terug te gaan in de tijd om ons die onbekende, piepende en zoemende machine voor de geest te halen waarvan we het fijne niet wisten, tot die slimme neef of oom een keer langskwam om het ding opgestart te krijgen en te laten zien waartoe die computer allemaal in staat was. De bewondering voor die ene kennis of dat familielid dat met een computer overweg kon, was nooit ver weg. Maar de grens

tussen bewondering en intimidatie is vaag. Wanneer je dus vandaag wordt aangesproken over phishing, reageer je soms even goedgelovig als vroeger in het bijzijn van die eerste computer.

De vissende hacker

De term phishing is gevallen en betekent vrij vertaald 'vissen'. En dat is het ook. Men vist. De hacker vist. De crimineel vist. Op een moment dat je het niet verwacht. Stel je dit even voor. Je gaat naar de supermarkt en neemt een winkelkarretje waarvoor je een muntstuk van een euro uit je portefeuille haalt. Ook de man naast je is op zoek naar kleingeld. Niet veel later kom je hem tegen terwijl je de vervaldatum van enkele producten bekijkt. De vriendelijke man verplaatst even zijn winkelkarretje en glimlacht minzaam. Jij glimlacht terug. De man maakt een opmerking over de vele producten waarvan de vervaldatum toch wel zeer dichtbij is. Jij maakt een soortgelijke opmerking. Er ontstaat een gesprek. De man wijst aan dat er iets hoger, verder dan jouw arm lang is, nog producten staan van recentere datum. Hij komt wat dichterbij en dat deert je niet, want er is een vorm van vertrouwen ontstaan. De man leunt tegen je aan en neemt een doosje van een hoge plank. Jij krijgt het aangereikt en bent hem dankbaar. Met het hartverwarmende gevoel dat er nog goede mensen bestaan, knik je de man toe alvorens verder te gaan met je boodschappen. De man moet er snel vandoor. 'Het werk wacht', zegt hij. Aan de kassa merk je dat je portefeuille weg is. Je bent bestolen door de vriendelijke man die bij de winkelkarretjes stuntelig zijn kleingeld zocht – om er op die manier achter te komen waar andere klanten hun portefeuille bewaren. Hij probeerde dat uit te vissen. Om niet veel later zijn hengel uit te slaan.

Phishing is een verzamelterm geworden voor de techniek waarbij criminelen proberen cruciale informatie te achterhalen,

die hen in staat stelt mensen te bestelen. In een digitale omgeving is het veel eenvoudiger om een valse identiteit te creëren dan in de oude vertrouwde fysieke wereld. Wanneer je een phishingmail krijgt waarin een interessant product voor een zeer gunstige prijs wordt aangeboden, en je klikt op de link in die mail om een aankoop te doen, dan heb je te goeder trouw een vals product in een valse winkel gekocht met echt geld. In de fysieke wereld is dat net iets moeilijker.

Neem nu de typische phishingmails waarin je voor enkele euro's een iPhone wordt aangeboden. De mail is zogezegd afkomstig van een bekende en betrouwbare winkel waarvan je de kleuren en het logo goed kent. In de mail staat het adres van een nieuwe vestiging van die winkel. Je stapt in je auto en rijdt ernaartoe. Je stapt de winkel binnen en het interieur lijkt als twee druppels water op dat van de winkel die je al kent. De man aan de kassa draagt exact hetzelfde uniform als de winkelier in de eerste winkel. Het doosje met de iPhone weegt precies zoveel als je zou verwachten en de verpakking ziet er vertrouwd uit. Maar bij thuiskomst stel je vast dat je 150 gram klei hebt gekocht. Je haast je terug naar de plek waar de winkel was, maar die blijkt spoorloos te zijn verdwenen. In de fysieke wereld is dit verhaal ongeloofwaardig, maar digitaal is het een fluitje van een cent om dit soort illusies te creëren. Hackers maken daarbij gebruik van software die hen in staat stelt om in enkele seconden een volledig waarheidsgetrouwe kopie te maken van een bekende webshop. De meeste phishingcampagnes zijn niet langer dan een uur actief. Binnen dat uur worden er zo veel mogelijk slachtoffers gemaakt. Daarna is er geen spoor meer van terug te vinden. Weg is de winkel, weg is de dief. En ook je geld.

In gewonemensentaal graag

Gelukkig bestaan er tal van initiatieven om mensen te wijzen op de gevaren van cybercriminaliteit. Veel van die campagnes geven tips voor het herkennen van phishingmails en proberen je te overtuigen van het nut van een wachtwoordbeheerprogramma. Maar toch weten veel mensen nog steeds niet goed waar te beginnen. Zo stelde ik na een infoavond over internetfraude vast dat heel wat toehoorders enthousiast waren over de opgedane kennis, maar toch achterbleven met vragen over wat ze straks thuis konden ondernemen om hun digitale gedrag echt veiliger te maken. Hoe begin je eraan? Welke stappen moet je zetten? En waar moet je dan op letten? Allemaal heel terechte vragen.

Ik merkte dat het aanbod van initiatieven om mensen in gewonemensentaal te helpen met soms ingewikkelde technische kwesties heel beperkt was. Zelf circuleer ik al enkele tientallen jaren in de wereld van computers en het internet. Ik heb al zo vaak mensen met hun digitale vragen moeten helpen, dat ik inmiddels over een behoorlijk arsenaal aan tips en bevattelijke metaforen beschik, die mensen doen begrijpen waar het nu eigenlijk om draait. Dat begrip is essentieel, want in de hele wereld van informatica en internet is iedereen het erover eens waar de zwakste schakel zich bevindt. Precies: bij de gebruiker zelf! In vakjargon hebben we het dan over de *human firewall*. Een firewall, letterlijk vertaald 'brandmuur', is in de informaticawereld het beveiligingstoestel dat de communicatie tussen computers nauwlettend in de gaten houdt en ingrijpt wanneer iets niet helemaal volgens de regels verloopt. Helaas kan zo'n firewall onmogelijk alle onheil voorkomen, aangezien het vaak niet de computers zijn die in de fout gaan, maar wel Frieda of Dirk die op hun bureaustoel een phishingmail vertrouwen en zich in de luren laten leggen. Omdat de zwakste schakel in het hele cyberverhaal de mens zelf is, vind ik het uitermate

belangrijk om iedere internetgebruiker te wapenen met de kennis die hem of haar in staat stelt zelf te fungeren als een 'menselijke' firewall.

Dit boek geeft je duidelijke antwoorden in de vorm van dertig tips die je, eventueel verspreid over dertig dagen, in de praktijk kan brengen. Na die ene maand zal je tot de tanden gewapend zijn tegen het gros van de cybercriminelen. Moeilijk is het niet, dat merk je meteen. Je kan de tips in dit boek in om het even welke volgorde toepassen. Ze staan allemaal los van elkaar. De ene is al wat eenvoudiger dan de andere. Sommige zullen, afhankelijk van jouw specifieke situatie, omslachtiger zijn en meer tijd in beslag nemen, maar elk van de tips kan je thuis zelfstandig in de praktijk brengen, zonder dat je daar iemand voor nodig hebt. Want als er iets is wat je ondertussen hebt geleerd, dan is het wel dat je niet om het even wie aan je digitale gegevens mag laten morrelen... Net zoals je geen dokter hoeft te zijn om beter voor je lichaam te zorgen, hoef je ook geen IT-specialist te worden om je gedrag op het internet beter te beveiligen.

Ook al pas je maar één of enkele van de dertig tips toe, elke stap is er een in de goede richting en maakt van jou een minder gemakkelijk doelwit voor cybercriminelen, zodat je naar hartenlust van de mogelijkheden van het internet kan blijven genieten. Immers, als je in het station een waarschuwingsbericht over zakkenrollers hoort, peins je er toch ook niet over om voortaan maar niet meer per trein te reizen?

Aan de slag!

www.standaarduitgeverij.be
info@standaarduitgeverij.be

www.stopphishing.be
www.nicojoos.be
www.katrienvaneffelterre.com

Vertegenwoordiging in Nederland
New Book Collective, Utrecht
www.newbookcollective.com

Eerste druk mei 2024

Ontwerp omslag en binnenwerk: Armée de Verre Bookdesign

ISBN 978 90 223 4110 0
D/2024/0034/126
NUR 740