HACKERS, PHISHING IDENTITEITSFRAUDE...

SAFETY FIRST ONLINE

De sleutel van je huis geef je niet aan een vreemde, maar online zijn we een stuk minder alert. Steeds meer mensen worden het slachtoffer van cybercriminaliteit. Eerst even dit lezen dus, vóór je online cadeautjes begint te shoppen.

DOOR **EVELIEN RUTTEN**.

De hacker heeft een compilatie gemaakt van de pornobeelden die ik bekeek én beelden van mijn naakte zelf. En hij vraagt geld...

Ik word wakker van een rare droom en grijp slaperig naar mijn smartphone. Ik open mijn mailbox en zit meteen rechtop in bed. Bij 'onderwerp' zie ik namelijk het wachtwoord staan dat ik een decennium lang heb gebruikt voor allerhande websites en mijn e-mailadres. Inmiddels heb ik het aangepast, maar die oh zo bekende combinatie van cijfers en letters open en bloot zien staan, geeft me rillingen. Ik heb een droge mond terwijl ik de mail openklik. Die begint zonder aanspreektitel: 'I'll get straight to the point'. De anonieme schrijver maakt mij er in perfect Engels op attent dat ik naar een geïnfecteerde pornosite ben gesurft. Ik denk even na, want porno interesseert me maar matig. Maar dan gaat er een lichtje branden. Natuurlijk! Een jaar geleden maakte ik een reportage over vrouwvriendelijke porno en daarbij hoort uiteraard research. Blijkbaar is er toen een bug in mijn laptop geïnstalleerd waardoor een hacker toegang kreeg tot mijn camera. Daarna zijn compromitterende beelden van mij gemaakt. Dat kan kloppen, want die laptop staat altijd open en ik werk thuis, de kans dat ik af en toe naakt door het beeld ben gewandeld, is groot. De hacker beweert dat hij een compilatie heeft gemaakt van de pornobeelden die ik bekeek én beelden van mijn naakte zelf. Als ik binnen de vierentwintig uur geen 3.500 euro in bitcoins stort, zal het filmpje naar al mijn contacten worden gestuurd. Ik spurt de slaapkamer uit en hap naar adem. Blinde paniek. Wat nu? Betalen? Niet betalen? Heb ik een garantie dat de chantage daarna ophoudt? Misschien moet ik gewoon een mail sturen naar iedereen die ik ken en uitleggen wat er is gebeurd en hopen dat vierentwintig uur later niemand die beschadigende mail open klikt?

Maar dan komen mijn razende gedachten tot stilstand. Wacht eens even. Als de hacker, die me de stuipen op het lijf heeft gejaagd met mijn oude wachtwoord, effectief bezwarend materiaal heeft, waarom toont hij dat dan niet gewoon met een demo-filmpje? Is dit wel echt? Ik kopieer de eerste paragraaf van de mail en plak hem in Google. Onmiddellijk krijg ik een lange lijst artikels te zien waarin deze methode wordt afgedaan als scam. Ik ben dus niet de enige die zich kapot geschrokken is. Het advies is duidelijk: niet betalen. Maar waar komt dat wachtwoord dan vandaan? Het antwoord is onthutsend: enkele jaren geleden zijn enkele grote databases (o.a. LinkedIn) gelekt en miljoenen mailadressen - inclusief de wachtwoorden - liggen nog steeds te grabbel voor iedereen die het interesseert. Dan is het gewoon een kwestie van copy/paste en hup: afpersingsmails à volonté. Vierentwintig uur later hou ik mijn mailbox angstvallig in het oog: zou het toch niet... Maar mijn vrees is ongegrond, er gebeurt niets. Ik delete de mail en plak een stuk witte tape over de camera van mijn laptop. *Just in case.*

IEDEREEN DOET HET, DUS...

De weken daarna stel ik me steeds meer vragen over mijn eigen online gedrag. Ik heb namelijk geen flauw benul van de risico's die ik loop. De digitale revolutie is doorgedrongen tot in de verste uithoeken van ons leven. We staan er niet meer bij stil dat onze privacy een lachertje is en hebben een vals gevoel van veiligheid. Twintig jaar geleden was telefonisch bankieren met de vaste lijn al supermodern, vandaag vinden we het

doodnormaal om onze bankrekening te checken op de smartphone en al wandelend naar de tram een betaling uit te voeren. Beveiligde wifi of niet. Terwijl we vroeger naar het reisbureau trokken om een voordelige vakantie te boeken, regelen we dat nu gewoon zelf online: van de huurauto en de vlucht tot het hotel. In plaats van ons in het gewoel van de winkelstraat te begeven, bestellen we die mooie laarzen wel via een Amerikaanse site en typen we zonder aarzelen onze kredietkaartgegevens in. Allemaal onder het mom van 'het zal wel veilig zijn, want iedereen doet het'. Maar helaas. Het is niét veilig. Volgens de meest recente cijfers waren er in 2017 in ons land bij de FOD Economie 9.000 meldingen van online fraude. In 2016 waren dat er nog maar 6.000. In 64 % van de gevallen levert een klacht niets op: de daders blijven onvindbaar (*Bron: De Tijd*).

SLECHTE VRIENDEN OP FACEBOOK

Zelfs als je profiel privé is, gebruiken fraudeurs slinkse technieken om je gegevens (naam, e-mail, wachtwoord, kredietkaartnummer) te pakken te krijgen. Met die gegevens kunnen ze onder jouw naam aankopen doen, een bankrekening openen, een telefoonabonnement afsluiten, een lening aangaan of illegale zaken doen. Let op voor de klassieke links waar vaak op geklikt wordt: het zijn valkuilen waardoor fraudeurs toegang krijgen tot je profiel en het risico op misbruik toeneemt:

"Want to know who viewed your account?"
"Your account is cancelled, please confirm your e-mail account"
"Earn loads of money working from home"
"Help, I'm in trouble"
"Is this you in this video?"

Bron: europol.europa.eu

AL JE WACHTWOORDEN OP STRAAT

Een telefonisch gesprek met **Patrick de Brouwer**, *ethical hacker*, is een eyeopener. "Op mijn 15de kwam ik in aanraking met het hackerswereldje, maar in 2010 behaalde ik de zwaarste certificeringen in security, waardoor ik een carrière aan de goede kant kon beginnen." Tegenwoordig werkt hij bij **Northwave**, een Nederlands IT-securitybedrijf dat op technisch en managementvlak bedrijven helpt om hun beveiliging naar een hoger niveau te tillen. De Brouwer heeft de taak om doelbewust aanvallen van buitenaf te doen. "Als een bedrijf in de jaren 90 een hacker inhuurde, was dat een groot schandaal. Nu schreeuwen ze erom, want ze kunnen zichzelf niet beschermen." Ik vraag De Brouwer in welke mate wij als particulieren voor cybercriminaliteit moeten vrezen. "Het ligt eraan hoe kwetsbaar je bent. Gebruik je hetzelfde wachtwoord op verschillende websites? Indien één van die sites wordt gehackt, zijn al je andere accounts ook niet langer veilig. Denk maar eens aan alle sites waar je online een aankoop hebt gedaan en je kredietkaartgegevens moest invoeren. Hackers die binnen je eigen systeem geraken, kunnen trouwens je toetsenbord uitzetten en de volledige controle overnemen. Een hacker kan bijvoorbeeld met een eenvoudig commando al je wachtwoorden zichtbaar maken en er een screenshot van maken." De Brouwer brengt dus geen goed nieuws. Het blijkt heel lastig om jezelf te beschermen tegen een cyberaanval. "Het is een kwestie van alertheid. Je moet veel behoedzamer omgaan met privé-informatie en mondiger worden. Als je twijfelt over een e-mail, bel dan naar de betrokken persoon en check

> 'Vroeger zag je aan het gebrekkige Nederlands of Engels dat een mailtje nep was. Vandaag huren ze professionele vertalers in'
>
> PATRICK DE BROUWER

BESCHERM JEZELF TEGEN HACKERS

1. Pas overal waar het kan de **'Two Factor Authentication'** toe. Daarbij moet je niet één wachtwoord ingeven, maar ook een tweede wachtwoord dat eerst naar je smartphone wordt gestuurd. Enkel als ze je computer én je telefoon in handen hebben, kunnen ze binnen raken.
2. Verander om de twee maanden van wachtwoord en gebruik niet voor elke site hetzelfde wachtwoord. Veilige wachtwoorden hebben minstens negen karakters en bevatten kleine letters, hoofdletters, cijfers en symbolen. Gebruik géén wachtwoorden die gebaseerd zijn op je persoonlijke leven (trouwdatum, naam huisdier...), want die kunnen hackers met een klein programmaatje eenvoudig achterhalen.
3. Update je internetbrowser regelmatig. Ze worden continu beveiligd op basis van de meest recente informatie over veiligheidsinbreuken. Maak ook af en toe een back-up van je volledige computer op een externe harde schijf die niet via wifi is verbonden met je computer. Bewaar die op een veilige plaats.
4. Gebruik **verschillende wachtwoorden** voor je persoonlijke en professionele accounts.
5. Sla nooit op je bureaublad een document op met daarin al je wachtwoorden. Gebruik in de plaats een password manager (bv. Password Boss of LastPass). Dat is een digitale beheerder voor al je wachtwoorden. Zelf hoef je dan nog maar één wachtwoord te onthouden: dat van de password manager zelf. Deze programma's worden heel grondig getest en zijn dus veilig.

Voor meer tips: safeonweb.be

of de mail wel degelijk van hem of haar afkomstig is. Krijg je een rare factuur, neem dan contact op met het bedrijf in kwestie. Helaas worden cybercriminelen steeds slimmer. Vroeger zag je meteen aan het gebrekkige Nederlands of Engels dat een mailtje nep was. Vandaag huren ze professionele vertalers in, zodat alles superprofessioneel lijkt."

HELP, DUBBELGANGER!

Een andere, ontwrichtende vorm van cybercriminaliteit is identiteitsdiefstal. **Inge** is gelukkig getrouwd, maar kreeg opeens rare signalen van haar beste vriend. "Hij vroeg me of alles goed was met mij en met mijn man. Huh?, dat wist hij toch?! Maar mijn vriend was net single geworden en zocht een nieuwe vriendin op Tinder. Daar was hij mij tegengekomen. Hij schrok en heeft 'mij' meteen weg geswipet. Op dit moment is er dus iemand aan het daten onder mijn naam en met mijn foto. Gewoon gestolen van Facebook. Krijg dat maar eens uitgelegd als vrienden of familie daarbij uitkomen." Ook **Dunya** heeft een schimmige dubbelganger. Ze

IS JOUW MAILADRES GEHACKT?

Surf naar**haveibeenpwned.com.** Typ je mailadres in en je krijgt meteen te zien of je nog veilig bent of niet. Verander sowieso regelmatig je wachtwoord.

GEEF JE NIET BLOOT!

Mail of text nooit intieme beelden van jezelf, ook niet naar iemand die je vertrouwt. Je weet namelijk nooit in wiens handen die smartphone of computer later terechtkomt. Vooral jongeren, die de impact van hun daden nog niet zo goed kunnen inschatten, sturen zonder nadenken intieme foto's van zichzelf en worden daardoor vaak afgeperst.

> "Op dit moment is er iemand aan het daten onder mijn naam en met mijn foto. Gestolen van Facebook"
>
> INGE

woont al vijfentwintig jaar in België en heeft de dubbele nationaliteit: Belgisch én Russisch. Ze is getrouwd, heeft twee kinderen en woont in Gent. Deze zomer kreeg ze een brief van een incassobureau. Blijkbaar moest ze nog duizenden euro's betalen voor een achterstallige elektriciteitsrekening. "Het ging over een woning in Leuven, waar ik nooit heb gewoond. Ik moet nu bewijzen dat ik niet dezelfde ben als de persoon die er wel verbleef. Daarom ben ik bij de gemeente al verschillende attesten gaan halen die bewijzen dat ik al die tijd in Gent heb gewoond. Maar nu zeggen ze dat ik ook een tweede woning heb kunnen huren op mijn naam..." De Brouwer bevestigt dat het zeer lastig is om hier onderuit te komen. "Identiteitsdiefstal is een fluitje van een cent als ze een kopie van je identiteitsbewijs in handen krijgen. Huur je op vakantie een auto bij een schimmig bedrijf en moet je zowel je kredietkaart als je ID-kaart afgeven? Dan loop je dus al risico. Of ze halen die gegevens uit het oud papier dat je aan de straat zet."

Gelukkig neemt de overheid de nodige stappen in de strijd tegen cybercriminaliteit. In België werd in 2014 het **Centrum voor Cyber Security** (CCB) opgericht. Met ontwikkelingen als Smart Industry, Internet of Things en 'in the cloud' werken is controle en veiligheid een must. Het CCB ontwikkelde een online referentiegids met meer dan 150 cyberveiligheidsmaatregelen om Belgische bedrijven te helpen beschermen tegen online aanvallen. Er is ook een sensibiliseringsprogramma voor het grote publiek. Elk jaar in oktober vindt de **European Cyber Security Month** plaats, waarbij de focus wordt gelegd op voorlichting. Nu maar hopen dat we de hackers te slim af blijven. ●

VISSEN NAAR JE GELD

Internetbankieren is absoluut veilig. Zeker als je met een kaartlezer een extra code moet ingeven. Maar **door middel van phishing kunnen cybercriminelen op een slinkse manier toch aan je geld komen**. Je krijgt bv. een mail die van je vertrouwde bank lijkt te komen. Een bediende vraagt om je rekeningnummer en code te herbevestigen, omdat je rekening anders niet meer veilig is. Ga je daarop in, dan kunnen hackers in een mum van tijd je rekening leegroven. Er zijn ook twee nieuwe vormen van phishing, namelijk *smishing* (via sms) en *vishing* (via een voice call, een telefoongesprek dus).
Slachtoffer van phishing?

- **Schakel je internetverbinding meteen uit** en gebruik een virusscanner om je computer én geheugenschijven te scannen.
- **Maak met een andere computer meteen nieuwe log-ins en wachtwoorden aan**.
- **Verwittig iedereen dat je slachtoffer werd van phishing** en dat ze moeten opletten met vreemde mails die van jou lijken te komen.
- Geef het misbruik aan bij het **Centrum voor Cyber Security België (CCB)** via verdacht@safeonweb.be.
- Als je gegevens geblokkeerd zijn door een virus en je het bericht krijgt dat je moet betalen om weer toegang te krijgen, ben je **het slachtoffer van ransomware**. Betaal nooit, want je hebt geen enkele garantie dat het daarna is opgelost. Neem hier ook contact op met het CCB.

Bron: secunews.be