Vijftig punten en tips waar je online echt iets aan hebt.

Je online veiligheid weer een beetje veiliger.

DENOUDEN
INFORMATIEBEVEILIGING
beschermt uw informatie

Naam document
Vijftig punten en tips waar je online echt iets aan hebt.
Auteur
Jochen den Ouden, Den Ouden Informatiebeveiliging / www.denoudeninformatiebeveiliging.nl
Versienummer
3.0
Versiedatum
November 2020
Versiebeheer
Het beheer van dit document berust bij Den Ouden Informatiebeveiliging.
Copyright

Rechten en vrijwaring

Inhoudsopgave

Voorwoord: De vijftig punten waar je online echt iets aan hebt.

Na de lezingen (en webinars) over cybercrime, informatiebeveiliging of online fraude kwamen steeds vaker vragen of er niet een lijstje was met tips en tricks om thuis nog eens na te lezen. Natuurlijk zijn er de hand-outs van die bij de lezing horen maar inderdaad, een lijst is nog veel handiger. Daarom hebben we een lijst samengesteld waar je echt iets aan hebt!

Voor je ligt dus dé lijst met maar liefst 50 (en een beetje meer) tips om nog veiliger online te werken. Denk aan het updaten van je computer, je virusscanner en het gebruiken van goede wachtwoorden. Maar daar stopt het niet. We heb er ook een aantal handige websites bijgevoegd die je helpen veilig online te gaan en te blijven.

We wensen je veel succes en veel veilige online kilometers met deze tips, trucks en websites.

Jochen & Ryanne den Ouden
Den Ouden Informatiebeveiliging

Wachtwoorden

Je wachtwoord is misschien wel het belangrijkste middel om een website binnen te komen. Veel mensen gebruiken, helaas, te vaak hetzelfde wachtwoord voor alle websites die zij bezoeken. En ook vaak een gewoon “woordenboekwoord”. Die zijn dus zo gekraakt. Daarom hieronder een aantal wachtwoordtips. Verderop krijg je informatie over een “passwordmanager” (een digitale kluis voor al je wachtwoorden). Superhandig en ik gebruik ‘m zelf ook.

1. Heb je voor alle verschillende websites een ander wachtwoord?

2. Je wachtwoord is minstens 8 tekens groot. Dit is echt minimaal. Echt goede wachtwoorden zijn minstens 20 tekens groot. Dat lijkt veel, maar bedenk je dat hoe kleiner je wachtwoord, hoe makkelijker het is voor iemand om hem te hacken.

3. Een wachtwoord kun je ook vervangen door een wachtzin. Dit is een "wachtwoord" met verschillende woorden. Een hacker kan deze veel moeilijker ontcijferen. Heel veilig dus.

4. Voorheen was het de bedoeling je wachtwoord vaak te wijzigen. Dat hielp eigenlijk niet want mensen zijn niet zo creatief als het op wachtwoorden aankomt. Je krijgt dan wachtwoorden als “Welkom01”, “Welkom02”, enz. Beter is het om een complex wachtwoord (of zin) te gebruiken, deze op te slaan in een password manager (zie punt 5) en te controleren of het gekozen wachtwoord in een database van gelekte wachtwoorden voorkomt (dat doen de managers hieronder maar je kunt het zelf ook doen met behulp van punt 7).

5. Om al die wachtwoorden te onthouden gebruik je een password manager. Voorbeelden hiervan zijn Dashlane (https://www.dashlane.com/nl) en Last Pass (https://www.lastpass.com/nl). Ook bestaan er open source alternatieven, zoals Keepass (https://www.keepass.info) en Bitwarden (https://www.bitwarden.com).

6. Waar het kan gebruik je twee-traps verificatie (two-factor authenticatie). Hier vind je meer informatie: https://veiliginternetten.nl/themes/situatie/wat-tweestapsverificatie/

7. Bang dat je wachtwoord gestolen is? Dan kijk je op de website https://haveibeenpwnd.com. Ja, dat is veilig.

Over je computer

Met je computer (en of dat nu een laptop of een desktop is) ga je online. Je doet je bankzaken ermee of je doet gewoon lekker iets met sociale media. Je moet er dus voor zorgen dat je computer in optimale conditie is om zich te wapenen tegen alle cyberboeven en vervelende malware.

Tips:

8. Zorg dat je computer altijd up-to-date is. Hoe je dit doet vind je voor Windows hier https://support.microsoft.com/en-us/help/12373/windows-update-faq en voor Mac hier: https://support.apple.com/nl-nl/HT201541

9. Na het updaten van je computer herstart je de computer. Zeker met een Windows computer is dit nodig omdat anders de updates niet juist zijn geïnstalleerd.
10. Je virusscanner (soms ook malwarescanner genoemd) is up-to-date. Zo krijg je minder snel een virus.

11. Zorg dat de virusscanner automatisch scant maar doe het zelf ook regelmatig, bijvoorbeeld 1 keer per week.

12. Zet je firewall aan. Standaard staat deze van Windows aan, maar je kunt ook een andere installeren.

13. Zorg voor een back-up. Dit kan in de Cloud (bijvoorbeeld met Dropbox) of op een andere harde schijf. Zorg dat je dan de schijf ergens anders bewaart, zodat bij bijvoorbeeld een brand je back-up veilig is.

14. De back-up van belangrijke documenten doe je het liefst zo snel mogelijk (dagelijks of op zijn minst wekelijks).

15. Je kunt je bestanden op de computer versleutelen. Op Windows kan dit via Bitlocker en met de Mac doet je dit met Filevault. Dit zorgt ervoor dat als je bijvoorbeeld je laptop kwijtraakt niemand je bestanden in kan zien. Je moet namelijk eerst een code invoeren voordat de bestanden zichtbaar worden. Hier vind je de uitleg van Bitlocker:

    https://support.microsoft.com/nl-nl/help/4028713/windows-10-turn-on-device-encryption

    en hier vind je die van Filevault:

    https://support.apple.com/nl-nl/HT204837

16. Vergrendel altijd je computer als je van je werkplek weggaat. Dit doe je onder Windows met de toetscombinatie Windows Toets + L. Je kunt het ook je schermbeveiliging zo instellen dat deze na verloop van tijd (bijvoorbeeld vijf minuten) automatisch de computer vergrendelt. Je doet dat zo:

    https://support.microsoft.com/nl-nl/help/4028111/windows-lock-your-windows-10-pc-automatically-when-you-step-away-from

E-mail en phishing:

Verreweg de meeste virussen (en andere malware) komen binnen via e-mail. Het is dus verstandig een gezonde dosis argwaan te kweken als je een mailtje krijgt die je niet vertrouwt. Hieronder vind je de tips weer:

17. Je klikt niet op mails die je niet kent.

18. Krijg je een mail van iemand die je wel kent maar vertrouw je het niet dan klik je niet op de links in de mail maar bel je de afzender even eerst. Zo controleer je of de mail die aan je verzonden is ook echt voor je bedoeld is. Toch zelf controleren? Doe dat met https://checkjelinkje.nl.

19. Een bijlage kan een virus bevatten. Zorg dat je dus zeker weet dat de bijlage die je krijgt door jou ontvangen had moeten worden. Checken of de veiligheid van een bijlage kan ook online: https://virustotal.com.

20. Je weet dat de bank nooit zo maar je PIN-code vraagt. Hetzelfde geldt voor de signeecode, een creditcard code of veiligheidscode van je creditcard. *Bij twijfel: hang op en bel de bank.*

21. Meld je af voor ongevraagde mails en nieuwsbrieven. Zo blijft je postvak schoon en behoud je het overzicht.

22. Als een e-mail van bijvoorbeeld de bank begint met "beste ontvanger", "geachte lezer" of iets dat daar op lijkt dan is het waarschijnlijk spam of een phishing mail. Bel in dit geval altijd met de bank. De bank zal namelijk altijd met Geachte heer/mevrouw <en dan je achternaam> beginnen.

23. Wanneer je een mail ontvangt en je bent er niet zeker van of het een betrouwbare mail is, probeer dan eens te zweven met je muis over de afzender. Hier zie je dan zijn e-mailadres. Check of dit inderdaad het emailadres is wat je verwacht.

24. Een ander veel gebruikte tactiek in phishing mails is de dwingende toon: je moet nu, direct en meteen iets doen. Als dit gebruikt wordt in een e-mail is het vaak een phishing mail.

25. Kijk ook uit met spookfacturen. Wees er zeker van dat een factuur klopt. Ook nu geldt: bij twijfel bellen.

Websites

Wat doe je eigenlijk niet online? Alles toch? Bankzaken, even een pizza bestellen, sociale media, een reis boeken. Alles! Maar bedenk je altijd: er kan iemand uit zijn op je creditcard gegevens of de gegevens die je invult voor een bestelling. Bekijk onderstaande tips en doe er je voordeel mee:

26. Je controleert of de website waar je naartoe gaat de juiste is. Controleer dus altijd het webadres.

27. Veilig internetten start met https:// en niet met http:// (zonder de S van secure). Daar let je dus op.

28. Vaak werkt een site prima zonder de cookies te accepteren. Accepteer daarom niet zondermeer de cookies.

29. Gebruik een pop-up blocker in je browser. Hoewel veel moderne browsers dit al tegenhouden kun je ook betere extensies downloaden voor je browser.

    Voor Chrome:
    https://chrome.google.com/webstore/detail/pop-up-blocker-for-chrome/bkkbcggnhapdmkeljlodobbkopceiche

    Voor Firefox:
    https://addons.mozilla.org/nl/firefox/addon/poper-blocker-pop-up-blocker/

30. Veel malware komt binnen via advertenties via websites. Een ad-blocker kan helpen dit tegen te gaan.

    Deze bijvoorbeeld: https://github.com/gorhill/uBlock#installation

Mobiele telefoons en wifi onderweg

Natuurlijk zijn we veel onderweg en dan gaat je mobiele telefoon ook mee. Cybercriminelen en andere boeven zijn ook online en stelen maar wat graag de data die je verwerkt met mobiele telefoon.

Hieronder de tips voor onderweg:

31. Ook je telefoon vergrendel je. Voor zowel Android toestellen als Apple toestellen is het verstandig een cijfercode (en het liefst in combinatie met een vingerafdrukscanner of gezichtsscanner) te gebruiken.

32. Open deur natuurlijk: laat je spullen nergens zomaar achter. Dat doe je nooit, toch? Dat betekent dat je ook je laptop uit de auto haalt wanneer je ergens naartoe gaat.

33. Ben je onderweg? Gebruik dan liever geen open Wifinetwerk. Hier kan iedereen op internetten dus ook de hacker. 4G is tegenwoordig in de gehele Europese Unie gratis wanneer het binnen je bundel valt. Probeer dus zoveel mogelijk met 4G te doen.

34. Wanneer je 4G gebruikt, kun je een hotspot maken met je telefoon. Zo kun je ook met je laptop online via je 4G bundel. Voor iPhones vind je hier de handleiding: https://support.apple.com/nl-nl/HT204023 en voor een Android toestel hier: https://www.androidauthority.com/mobile-hotspot-setup-631280/

35. Kan het toch echt niet anders? Zorg dan dat je het wachtwoord gekregen hebt van de plek waar je internetten wilt en doe geen bankzaken en verstuur geen persoonlijke gegevens over het netwerk.

36. Gebruik, zeker onderweg, een Virtual Private Network (VPN). Dit is een veilige "tunnel" waardoor een hacker niet bij je data kan die verzonden wordt. Veel gebruikten VPN's zijn:
    - https://nld.privateinternetaccess.com/
    - https://nordvpn.com/nl/

    Gebruik liever geen gratis VPN. Deze verkopen je privéinformatie maar wat graag en dan heeft het hele nut van een VPN weinig zin.

37. Verwijder wifinetwerken die je niet meer gebruikt. Denk aan een netwerk van een hotel waar je ooit gebruik van gemaakt hebt.

38. Maak je onderweg gebruik van iemand anders zijn of haar computer? Of bijvoorbeeld van de computer in een hotel? Zorg dat je altijd uitlogt en verander na afloop je wachtwoorden. Doe er liever ook geen bankzaken mee. Gebruik de privé-tab in de browser.

39. Deel niet constant je locatie. Veel applicaties (apps) op je telefoon delen je locatie. Dit is niet nodig, verbruikt veel stroom van de accu en het is onveilig.

40. Een nieuwe app? Bekijk dan wat de app allemaal kan delen? Je locatie is er een maar ook bijvoorbeeld je contacten of chatgeschiedenis. Deel alleen wat je wilt. In de instellingen van de app of de telefoon zelf kun je aangeven wat je wilt delen.

41. Apps downloaden en installeren doe je alleen vanuit de officiële app stores. De kans dat je een met malware geïnfecteerde app download is groot als je dit zo maar ergens vandaan haalt.

Thuis en routers

Ben je weer thuis? Dan wil je ook dat je wifi veilig is en dat niet iedereen daar zo maar gebruik van kan maken. Controleer je eigen wifi-router met de volgende handige tips:

42. Beveilig ook je router: update deze regelmatig.

43. Zorg dat je router een goed (sterk) wachtwoord heeft zodat niet iedereen er zomaar in kan.

44. Gebruik je geen gastennetwerk en laat je niemand van buiten op je netwerk? Zet dan het gastennetwerk uit.

45. Heb je weleens gasten en wil je hen ook gebruik laten maken van het netwerk (wifi) zorg dan dat je je gastennetwerk juist aanzet. Zijn je gasten weg? Zet dan je gastennetwerk weer uit. Sommige routers laten je zelfs een bepaalde tijd je gastennetwerk in de lucht houden (bijvoorbeeld twee uur) daarna zorgt de router zelf dat het gastennetwerk uit gaat.

46. Kijk regelmatig welke apparaten er verbonden zijn met je router. Doe dit bijvoorbeeld 1 keer per maand. Zitten er apparaten tussen die je niet kent? Verwijder deze en kies een nieuw wachtwoord voor je router en het verbinden.

47. Verander ook van je router regelmatig het wachtwoord. Zowel voor de wifiverbinding als het beheersysteem van de router.

Delen en USB-sticks

Het is met een computer, je tablet of mobiele telefoon nog nooit zo makkelijk geweest om even snel een document met iemand te delen. Maar je deelt al snel te veel of je ontvangt software die je eigenlijk niet wilt, zoals een virus. Daarnaast: een USB-stick is makkelijk maar je verliest ze ook snel. Hoe deel je nu wel slim en makkelijk? Bekijk de zinvolle tips hieronder:

48. Een USB-stick kan handig zijn, maar kun je verliezen. Beter zet je hier dus geen persoonlijke gegevens op.

49. Een geïnfecteerde (foute) USB-stick kan zorgen voor malware zoals een virus op je computer. Iemand die je dus een stick uitleent kan deze dus (opzettelijk) besmet hebben. Kijk hier mee uit.

50. Deel je weleens iets via een clouddienst zoals bijvoorbeeld Dropbox of OneDrive? Doe dit dan met een wachtwoord. Het wachtwoord verstuur je via een SMS of Whatsapp naar de ontvanger. Zorg ook dat het gedeelde document na een paar dagen/weken weer ongedeeld wordt. Zo voorkom je dat iemand anders dan de ontvanger (degene met wie je deelt) de bestanden ontvangt of kan downloaden.

51. Deze geldt eigenlijk overal: klik niet zomaar op de "Ik ga akkoord". Je deelt al snel veel te veel informatie.

Social Media

Over delen gesproken: je leven deel je misschien ook online. Ik begrijp ook dat dat leuk is, maar het kan ook onveilig zijn. Daarom heb ik een paar tips opgesomd die je helpen veiliger online te zijn met sociale media.

52. Contacten die je zomaar een aanbieding doen via bijvoorbeeld een instant messenger (Facebook Messenger of Instagram)? Dit kan een vorm van phishing zijn. Bel het contact om te verifiëren dat dit echt is.

53. Gebruik altijd je gezonde verstand. Ziet iets er te mooi uit om waar te zijn? Dan is dit het waarschijnlijk ook.

54. Zet je profielpagina van Facebook op privé. Zo kunnen alleen je vrienden je profiel zien en niemand daarbuiten. Dit kan ook voor andere social mediasites zoals Instagram.

55. Bedenk goed wat je wel en niet online zet. Je deelt snel te veel. En weet ook met wie je dat deelt.

56. Marktplaats. Kopen gaat snel maar ook vaak onveilig. Probeer altijd een persoonlijke afspraak te maken. Zo kun je het product zien en dan de koop sluiten. Ook kun je gebruik maken van de gelijk oversteken service van Marktplaats (https://help.marktplaats.nl/help/veilig_handelen_internetoplichting/tips_voor_veilig_handelen/i/gelijk-oversteken)

57. Blokkeer ongewenste profielen.