Tips tegen hackers en oplichters

1. Check op https://haveibeenpwned.com of bedrijven/websites je wachtwoord gelekt hebben en zo ja, verander zo snel mogelijk je wachtwoord (ook op alle andere websites waar je dat wachtwoord voor gebruikt).

2. Bewaar je wachtwoorden niet in je computer. Goede apps die je wachtwoorden onthouden zijn Last Pass, KeePass en 1Password. Hiermee hoef je nog maar één wachtwoord te onthouden, die van de app zelf. Alle andere wachtwoorden worden door het programmaatje onthouden. Ze zijn beveiligd door sterke versleuteling (encryptie).

3. Verander geregeld je wachtwoorden en kies verschillende wachtwoorden voor belangrijke sites.

4. Gebruik in je wachtwoord zowel (hoofd)letters als cijfers en tekens. Maak het vooral zo lang mogelijk. Verleng je wachtwoord per site door iets van de site er aan toe te voegen (bijvoorbeeld Ma voor Marktplaats) of iets wat met de site te maken heeft, bijvoorbeeld Boeken bij Bol.com

5. Check of je antivirusprogramma up-to-date is. Negeer geen updates van programma's, ook al gebruik je ze niet vaak. Schakel de automatische updates van je antivirusprogramma in en laat het geregeld alle apparaten scannen op infecties. Schakel een eventueel meegeleverde firewall altijd in.

6. Verstrek een kopie van je legitimatiebewijs alleen als dat wettelijk verplicht is. Veel instanties mogen het helemaal niet vragen; dat geldt bijvoorbeeld voor hotels en sportscholen in Nederland. Alleen overheidsinstanties, werkgevers, zorgverzekeraars, notarissen en banken mogen vragen om een kopie van je paspoort. Toch zijn er heel veel andere bedrijven die dat doen, terwijl ze kunnen volstaan met het noteren van de gegevens. Meld dat soort overtredingen bij de Autoriteit Persoonsgegevens https://autoriteitpersoonsgegevens.nl

7. Plaats een aantekening op een kopie van je legitimatiebewijs waarvoor deze kopie bestemd is, bijvoorbeeld 'kopie voor autoverhuurbedrijf

Olymp'. Streep je burgerservicenummer op de kopie door (dat staat op twee plaatsen in je paspoort, ook in het lange nummer onderaan).

8. Download de gratis app KopieID van de Rijksoverheid om op een veilige manier digitale kopieën te versturen. Het werkt simpel.

9. Bewaar nooit kopieën van belangrijke documenten in je computer, beter op een usb-stick of een externe harde schijf, die je als back-up gebruikt.

10. Leeg geregeld de prullenmand van je computer, want documenten in je prullenmand blijven kwetsbaar voor virussen.

11. Op de site van de politie https://www.politie.nl/aangifte-of-melding-doen/controleer-handelspartij.html kun je checken of iemand als oplichter bekendstaat. Je kunt bankrekeningen, telefoonnummers en webadressen op betrouwbaarheid scannen. Een check op Google levert vaak ook klachten op als het om een onbetrouwbare aanbieder gaat. Ook op www.opgelichtopinternet.nl is veel informatie over oplichters en foute rekeningen te vinden.

12. Klik nooit op linkjes die je niet helemaal vertrouwt, zelfs niet als die afkomstig zijn van goede vrienden. Wees helemaal voorzichtig bij Engelstalige teksten, wenskaartjes en winacties.

Banken en andere financiële instellingen sturen je geen e-mails met vragen over persoonlijke gegevens. Als je zo'n e-mail ontvangt, kun je ervan uitgaan dat het om phishing gaat.

13. Heb je op het werk per ongeluk geklikt op een phishingmail? Meld het aan de ict-afdeling en zet je computer zo snel mogelijk uit (of log uit) om snelle besmetting van bestanden te voorkomen.

14. Gebruik geen Google, maar een zoekmachine die je digitale sporen niet opslaat, zoals DuckDuckGo of Epic, www.duckduckgo.com of www.epicsearch.in.

15. Wis apps die je niet langer gebruikt en wees op je hoede bij het downloaden van nieuwe apps, vooral als die gratis zijn. Er zijn apps die je hele mobiel leegtrekken. Bij sommige apps kun je de locatie en het delen van contacten uitzetten, zelfs achteraf. Facebook-apps verzamelen veel informatie over je, dus probeer het gebruik daarvan te beperken. Bij elke app zie je een knop 'Instellingen bewerken'. Als je erop klikt, kun je zien naar wie deze app posts verstuurt en wat die nog meer in jouw naam mag uitspoken. Vrienden maken ook van alles over jou openbaar door simpelweg Facebook-apps te gebruiken. Bij 'Apps die anderen gebruiken' kun je dat allemaal zien. Alle punten die hier aangevinkt staan, van je

biografie tot je statusupdates, worden te grabbel gegooid. Je kunt alle vakjes uitvinken als je op je privacy gesteld bent.

16. Installeer apps voor mobiel of tablet uitsluitend via de officiële app-stores. Gebruik geen illegale kopieën in verband met virussen. Kijk ook goed naar de toegangsrechten van de app en naar ervaringen van medegebruikers (lees dus de recensies voordat je een app downloadt).

17. Als je een computer buitenshuis gebruikt voor social media of internetbankieren, vergeet dan niet uit te loggen. Vink sowieso de functie om je wachtwoord te onthouden af. Sommige browsers onthouden je wachtwoord, dus wis voor de zekerheid de geschiedenis van de browser.

18. Via de site disconnect.me kun je voorkomen dat Facebook je activiteiten elders op het internet volgt.

19. Als je iets impulsiefs zegt op social media, wis het dan zo snel mogelijk. Zo blijft de schade beperkt.

20. Googel jezelf af en toe om je onlinereputatie te checken. Stel ook een Google Alert op je naam in zodat je een seintje krijgt wanneer er iets over je op het internet verschijnt.

21. Heb je een 'politievirus' of ander soort malware in je computer gekregen, kijk op de site van de politie hoe je die kunt verwijderen. Betaal in elk geval geen geld voor de verwijdering ervan, want zo sponsor je de criminelen http://www.politie.nl/onderwerpen/ransomware.html. Ook de sites waarschuwingsdienst.nl of fraudehelpdesk.nl helpen je verder.

Verwijder je verjaardag van Facebook. Heel veel datahandelaren zoals Experian, Acxiom en Rapleaf koppelen je 'likes' aan je geboortedatum en dan weten ze bijna zeker wie je bent.

22. Wees voorzichtig met je privégegevens en zet nergens op internet je 06-nummer en je geboortedatum.

23. Kinderen zijn heel scheutig met informatie over zichzelf, familie en vrienden. Ze zien de gevaren niet. Aan een onbekende op straat geven ze hun adres niet, maar op internet wel. Leer je kinderen om niet klakkeloos hun gegevens in te vullen op websites die dat vragen. Het enige wat echt moet kloppen is meestal het e-mailadres, want daar wordt je wachtwoord naartoe gestuurd. Je echte naam hoeven de sites niet te weten en je adres evenmin.

24. Beveilig je brievenbus, zodat criminelen niet je post kunnen stelen.

25. Gooi documenten met persoonsgegevens niet bij het oud papier. Koop een papierversnipperaar en haal alle documenten met vertrouwelijke informatie erdoorheen.

26. Gebruik programma's zoals Eraser, Sure Delete en Wipe Drive als je je harde schijf wilt wissen. Vernietig de harde schijf als je computer naar de vuilstort gaat.

27. Check voordat je iets bij een webshop bestelt of die goed uitziende webshop niet nep is. Zoek op reviews en ervaringen van andere consumenten. WebWinkelChecker http://webwinkelchecker.nl is een gratis hulpmiddel om te checken of anderen negatieve ervaringen met een webshop hebben. Het waarschuwt ook voor faillissementen en misbruik van keurmerken.

28. Werk voordat je online gaat winkelen of betalen je besturingssysteem bij met de nieuwste updates. Het gratis programma Scancircle https://www.scancircle.com/nl wordt aanbevolen door de Consumentenbond en laat zwakheden in je computer zien.

29. Het Centraal Meld- en informatiepunt voor Identiteitsfraude en -fouten (CMI), de Fraudehelpdesk en het Landelijk Meldpunt Internetoplichting geven voorlichting en helpen slachtoffers bij het doen van aangifte en bij het oplossen van problemen.

30. (Tips uit het boek 'Komt een vrouw bij de h@cker' https://www.bol.com/nl/f/komt-een-vrouw-bij-de-hacker/9200000022439329/ ;in het boek kun je lezen hoe hackers werken en hoe ver ze gaan. Achterin vind je een bijlage met nog meer handige tips).

Met vriendelijke groeten,

Maria Genova

www.mariagenova.nl

LinkedIn https://www.linkedin.com/in/maria-genova-528bb77?trk=hp-identity-name

Twitter: https://twitter.com/genova2

Facebook https://www.facebook.com/MariaGenovaBooks/?fref=ts