Transcipt De SeniorWeb Podcast

Zegert van der Linde in gesprek met Esther Mieremet

00:00:00

Zegert van der Linde: Welkom bij de SeniorWeb Podcast. Mijn naam is Zegert van der Linde. Fijn dat u luistert.

00:00:08

Zegert van der Linde: De maand maart staat bij SeniorWeb in het teken van veiligheid en privacy. In deze vier podcastafleveringen praat ik met verschillende gasten over dit thema. U krijgt achtergronden, verdieping en praktische tips om veilig online te gaan.

00:00:22

Zegert van der Linde: Welkom, Wachtwoord of 123456. Grote kans dat ik zojuist één van uw wachtwoorden heb voorgelezen. Dit zijn namelijk drie van de meest gebruikte wachtwoorden van Nederland, en dat is niet zo handig, want een uniek wachtwoord is de basis van al uw online veiligheid.

00:00:45

Zegert van der Linde: Vandaag zit tegenover mij Esther Mieremet zij werkt bij ECP, platform voor de informatiesamenleving, en is daar projectleider voor veiliginternetten.nl. Zij weet dus alles over back-ups maken, antivirussoftware en veilig inloggen. Welkom Esther.

00:01:02

Esther Mieremet: Dank je wel.

00:01:03

Zegert van der Linde: Heb ik jouw wachtwoord net voorgelezen?

00:01:09

Esther Mieremet: Zeker niet.

00:01:09

Zegert van der Linde: Nee, gelukkig maar.

00:01:09

Esther Mieremet: (lacht)

00:01:09

Zegert van der Linde: Anders had je hier niet moeten zitten denk ik.

00:01:09

Esther Mieremet: Dat denk ik ook, ja.

00:01:11

Zegert van der Linde: Het komende half uur wil ik een paar thema's belichten die een beetje te maken hebben met online veiligheid, te beginnen met software-updates. Waarom is het zo belangrijk om je software up to date te houden?

00:01:23

Esther Mieremet: Dat is belangrijk omdat er soms wat kleine foutjes in de software zitten en die worden dan hersteld. Dus wat er gebeurt op het moment dat je software op je laptop of je iPhone of welk device of apparaat je ook hebt, als dat geïnstalleerd is, kunnen hackers kleine gaatjes en foutjes vinden. En op het moment dat er een update is worden die hersteld. Dus eigenlijk ben je zo veilig mogelijk als je altijd de laatste update hebt.

00:01:53

Zegert van der Linde: Dat is dus eigenlijk dat de softwarefabrikant ontdekt dat het deurtje niet goed op slot zit. We zetten er nog even een extra slot op dus zorg dat jij hem geüpdatet hebt.

00:02:02

Esther Mieremet: Ja. Zeker, dat is het.

00:02:04
Zegert van der Linde: Soms hoor ik ook dat een bedrijf een bepaalde, verouderde versie van software niet meer ondersteunt. Zo las ik in januari dat Microsoft Windows 7 niet meer ondersteunt. Wat betekent dat?
00:02:16
Esther Mieremet: Ja, dat is eigenlijk het lastige van alle bedrijven. Bedrijven zijn natuurlijk commercieel, dus ze willen dat je overgaat naar een nieuwere versie en daar kunnen ze geld voor vragen. Dat is natuurlijk logisch en er wordt door de overheid heel veel gelobbyd om te zorgen dat ze zo lang mogelijk bestaande software ondersteunen. Dus als je iets koopt, dat je zo lang mogelijk garantie hebt dat het veilig is. Maar er worden ook nieuwe dingen ontwikkeld en dat betekent soms dat het voor een bedrijf niet rendabel is om het onder de ondersteuning van de oude dingen nog te doen. En daarom, op het moment dat er echt niet meer ondersteund wordt, moet je echt overstappen.
00:02:53
Zegert van der Linde: Stel dat ik bijvoorbeeld een laptop of een computer heb waar Windows 7 op draait. Wat moet ik dan doen?
00:02:58
Esther Mieremet: Wat je moet doen is naar Microsoft surfen en het nieuwe pakket aankopen. Dat is echt een heel simpele vraag. En vaak krijg je een melding dat de software verouderd is en dan wordt ook aangegeven welke stappen je moet ondernemen dus dan kun je gewoon volgen. Maar als je niet zeker weet of het echt nodig is dan kan je natuurlijk altijd bijvoorbeeld bellen met SeniorWeb of met iemand in de buurt om te vragen: 'is het echt nodig?', als je twijfelt.
00:03:27
Zegert van der Linde: Is het ook een veiligheidsrisico dan?
00:03:28
Esther Mieremet: Ja, want als er geen ondersteuning meer is dan zorgt de fabrikant er ook niet meer voor dat het veilig is. Dus die gaatjes die gevonden worden, die luikjes waar ik het net over had, die blijven dan bestaan en die kunnen groter worden.
00:03:41
Zegert van der Linde: Voor een tablet gebeurt het soms ook. Ik hoor ook weleens van apps die niet meer werken op een oude iPad ofzo. Waarom is dat dan?
00:03:49
Esther Mieremet: Ja, dat is echt wel omdat ze willen dat je een nieuwe iPad koopt.
00:03:54
Zegert van der Linde: Het is dus ook echt gewoon iets financieel?
00:03:56
Esther Mieremet: Ja, het is twee kanten op.
00:03:57
Zegert van der Linde: Als je dan je software geüpdatet hebt dan kan je online. Ik las een paar mooie basisregels, of eigenlijk één regel maar twee keer anders verwoord. De ene zegt: klik niet klakkeloos - heel veel K's - of, zoals jullie zeggen bij veiliginternetten.nl: eerst checken, dan klikken. Wat bedoelen jullie daarmee?
00:04:18
Esther Mieremet: Dat betekent dat als je een berichtje krijgt op welke manier dan ook - dat kan een e-mail, sms-je of whatsappje zijn met een link daarin, en een link zie je vaak met onderstreping, en als je erop kan klikken dan opent zich bijvoorbeeld een pagina. Op het moment dat je out of the blue een link krijgt met 'klik hierop', dan moet je je eigenlijk afvragen: waarom? Waarom krijg ik een link om op te klikken en van wie krijg ik die? Dat is het eerst checken, dus nadenken waarom je het krijgt. En als je het dan gecheckt hebt en denkt: oké, dit is logisch, ik moet iets doen, ik snap het en de afzender is ook wie ze zeggen dat ze zijn, dan kan ik erop klikken.
00:05:07
Zegert van der Linde: Maar dat is best wel lastig, want die mailtjes worden steeds beter naar mijn idee. Vroeger kon je

die spam-mailtjes met slecht Nederlands er zo uitpikken. Hele rare zinnen zaten daarin. Maar dat is niet altijd meer zo.

00:05:23

Esther Mieremet: Inderdaad, en dat is ook wat het lastig maakt. Want je zegt 'eerst checken', maar wanneer weet je of je het moet checken? Want dan moet je je dus bewust zijn dat je het moet checken. Het voelt soms ook een beetje argwanend hè, dat je altijd bij alles wat je krijgt moet bedenken of het wel juist is. Dat is natuurlijk ook niet echt een positieve manier van in het leven staan. (lacht)

00:05:48

Zegert van der Linde: Ja, dat is wel een beetje een vervelende gedachte. Dat je bij elke mail denkt: kan ik hier nou wel op klikken of niet?

00:05:48

Esther Mieremet: Ja, en wat je heel goed ziet is dat banken en ook overheidsinstellingen steeds beter communiceren dat ze je niet gaan mailen met een linkje. Dus op het moment dat je van de Belastingdienst, DigiD of banken een mailtje krijgt van: 'klik hierop' dan weet je eigenlijk bij voorbaat al dat je dat niet moet doen, want zij communiceren niet met linkjes waar je op moet klikken.

00:06:11

Zegert van der Linde: Dat is een hele goeie basisregel eigenlijk.

00:06:14

Esther Mieremet: Ja, en als er ook nog bijstaat dat je het snel moet doen dan weet je het wel zeker, want dan voel je de neiging tot urgentie, en als je dat voelt dan moet je niet klikken en dan kan je het beter nog even laten liggen en er de volgende dag nog eens naar kijken. En als je het dan nog eens bekijkt dan blijkt vaakt dat je denkt: ik denk niet dat het nodig is dat ik hierop klik.

00:06:40

Zegert van der Linde: En als je een mailtje krijgt van de bank dan kan je ook even naar de bank bellen. Vaak weten ze dan ook wel of een mail echt is of niet.

00:06:47

Esther Mieremet: Ja. En wat mensen ook heel vaak doen, is even googelen. Bijvoorbeeld 'phishing' of 'nepmail' en dan 'ING' of welke bank dan ook. En dan zie je meteen: 'klik hier niet op'. Dus eigenlijk weet je het dan al.

00:07:01

Zegert van der Linde: Ja. Ik weet dat SeniorWeb ook af en toe dit soort dingen deelt via de website, phishingmails die rondgaan. Dus dat kan je ook nog in de gaten houden. We hebben het nu over mailtjes en whatsappjes. Wat natuurlijk weleens een beetje gevaarlijk is daarin is dat je ook weleens berichtjes krijgt van vrienden of zo. Je hoort ook weleens van Whatsapp-fraude, waarbij je van een bekende een berichtje krijgt in de zin van: 'Hey, wil je me even 1500 euro overmaken want ik heb geld nodig.' Kan je dat op de een of andere manier herkennen?

00:07:40

Esther Mieremet: Ja... Ze noemen dat WhatsApp-fraude of vriend-in-nood-fraude, dus alsof iemand in nood is en vraagt: 'Help mij.' En omdat we als mens algemeen geneigd zijn elkaar te helpen - waarom zou je niet willen helpen - word je aangesproken op een bepaald gevoel. Dat doen die criminelen heel goed, om het maar even onaardig te zeggen. Je voelt dat je graag wilt helpen. En wat je eigenlijk altijd moet doen als je denkt dat je met een bekende aan het appen of sms-en bent, is diegene even bellen. Want als diegene aan de andere dan een andere stem heeft of niet opneemt, dan is het én niet urgent én waarschijnlijk niet diegene.

00:08:25

Zegert van der Linde: Dus dan is het waarschijnlijk gewoon nep. Geldt dat bijvoorbeeld ook als je op een website zit? Kan je op een website gewoon op alle linkjes klikken die er staan?

00:08:35

Esther Mieremet: Ja, als het een veilige website is. En of het een veilige website is, dat zie je boven in de browser. Als

je HTTPS ziet. Met een 's' is namelijk versleuteld. En dan zie je een URL, dus de naam van de pagina waar je bent, bijvoorbeeld seniorweb.nl. En als het dan bij wijze van spreken seniorenweb.nl is dan is het niet seniorweb.nl. En dat is natuurlijk wel heel tricky want dat is ook heel moeilijk te zien. Als het ingx.com is dan is het niet ing.com. Als het veiliginternette.nl is dan is het niet veiliginternetten.nl. Dus je moet kijken waar je bent, of het veilig is, en als je er dan bent en je krijgt 'klik hierop' te zien dan is het prima, want dan zit je in de veilige omgeving van die website. Maar je moet wel eerst op de juiste website zitten. Nog een tip daarbij is: op het moment dat je bijvoorbeeld in een nieuwsbrief een linkje krijgt naar een website, of je krijgt een mailtje met: 'klik hierop', en dan ga je naar de website. Dan kan je ook gewoon die website zelf intikken. Dus in plaats van op het linkje te klikken kan je ook gewoon zelf even seniorweb.nl invullen, want dan weet je zeker dat je naar de echte SeniorWeb gaat en via de link kan je soms wel naar een nep-seniorweb.nl gaan.

00:10:07

Zegert van der Linde: Maar als er dan staat 'kik hier' of 'hier' is het linkje waar je op moet klikken, dan weet je niet welke code ze erachter hebben verstopt.

00:10:08

Esther Mieremet: Ja, klopt. Als je trouwens gewoon de nieuwsbrief van SeniorWeb krijgt natuurlijk niet, omdat je specifiek hebt aangegeven dat je die nieuwsbrief wilt ontvangen. Maar als je een nieuwsbrief krijgt waarvoor je je nooit hebt opgegeven dan zou ik niet gewoon op de link klikken maar zelf even het adres invullen, en dan zie je wel vanzelf of je komt waar je moet zijn of niet.

00:10:31

Zegert van der Linde: Wat dan ook nog belangrijk is, is antivirussoftware. Waar beschermt die software ons tegen?

00:10:37

Esther Mieremet: Een virus is een aanval van buitenaf. Kijk maar naar corona, dat is ook een virus.

00:10:40

Zegert van der Linde: (lacht)

00:10:40

Esther Mieremet: Dat is dus een mooi voorbeeld. Maar dit is dus een virus op je computer. En het is wel zo dat heel veel programma's die je nu al op je computer hebt... Als je een laptop of een computer koopt en hij is geïnstalleerd dan zit er al automatisch virussoftware op hè. Bijvoorbeeld Microsoft en Apple hebben intern als virusscanners. En als je dan bij de instellingen aanduidt dat je automatische updates wilt dan moet je niet eens een extra pakket kopen want dan zit het er al in.

00:10:40

Zegert van der Linde: Oh, dat is nieuw voor mij.

00:10:40

Esther Mieremet: Ja, dus op het moment dat je een aanschaf doet, vraag dan gelijk bij de aanschaf of er in het systeem dat je koopt al automatisch virusscanners zitten. En tegenwoordig hoor je dan negen van de tien keer 'ja'.

00:11:33

Zegert van der Linde: Oh, wat goed.

00:11:34

Esther Mieremet: Vroeger - pakweg tien of zeven jaar geleden - moest je nog echt een antiviruspakket kopen.

00:11:40

Zegert van der Linde: Maar is dat dan niet beter?

00:11:42

Esther Mieremet: Nee, dat is niet beter.

00:11:45

Zegert van der Linde: Dus de gewone standaard virussoftware van Microsoft of Apple is gewoon goed.

00:11:47

Esther Mieremet: Ja, die is goed genoeg en die beschermt jouw systeem, zoals dat heet.

00:11:52
Zegert van der Linde: Oké. En moet je die dan ook weer updaten?
00:11:52
Esther Mieremet: Als je het aanzet dan doet die dat automatisch. Dus als je bij de instellingen kiest voor 'automatische updates' dan doet die dat automatisch.
00:11:52
Zegert van der Linde: Ideaal. Nooit meer over nadenken.
00:12:04
Esther Mieremet: Nee, want die bedrijven willen ook dat hun producten zo veilig mogelijk zijn, want dan worden ze meer gebruikt en dan hebben ze ook minder gedoe. Dus zij hebben er ook baat bij, en ze werken ook mee aan heel veel campagnes om ervoor te zorgen dat mensen zich zo veilig mogelijk kunnen bewegen op het internet.
00:12:21
Zegert van der Linde: Ik weet nog van pakweg vijftien jaar geleden dat je je computer af en toe helemaal moest scannen met software. Je moest hem dan aanzetten en dan ging die alle bestanden langs die op je computer stonden, wat soms drie uur duurde, en dan ging die checken of er ergens een virus inzat. Moet ik dat nog steeds handmatig doen?
00:12:43
Esther Mieremet: Dat moet nog steeds, maar dat hoeft ook niet handmatig. Want als je instelt dat je een automatische update doet voor je updates, maar ook een automatische virusscan dan doet die dat gewoon zelf, en dan krijg je meestal rechtsonder of rechtsboven een berichtje van: 'ik check hem even', en dan gaat hij het checken. Dat duurt gelukkig ook geen uren meer tegenwoordig maar je moet dan ondertussen wel even een kopje koffie halen ofzo. Het is niet zo dat het gelijk gedaan is. En als je het ook regelmatig doet of als het regelmatig gebeurt dan is het ook korter, laat ik het zo zeggen. Als je het uitzet omdat je er geen zin in hebt, en dat hebben we wel hé. Je moet snel even een mailtje sturen en dan denk je: daar heb ik nu even geen zin in. Maar als je dat natuurlijk de hele tijd niet doet dan ben je ook de hele tijd niet meer op het beste beveiligingsniveau. Dus wees af en toe ook wat kritisch naar jezelf en neem dan heel even de tijd.
00:13:15
Zegert van der Linde: Dan ga ik wel even koffie drinken of een berichtje sturen via mijn telefoon ofzo.
00:13:41
Esther Mieremet: Ja, of 's nachts of 's avonds updaten.
00:13:47
Zegert van der Linde: Ja, dat is ook handig. Ik heb nog wel een extern pakket op mijn laptop staan en die scant volgens mij ook alle bestanden die ik download. Als ik op internet een programma download voor het een of ander dan scant die het ook gelijk even, van: 'hey, is dit goed? Ja, het is goed. Je kan het openen.' Dat bieden ze ook steeds meer aan. Bijvoorbeeld ook als je een bijlage krijgt in een mail dan scant ie dat ook automatisch.
00:14:13
Esther Mieremet: Ja. Het is wel zo dat als het een goeie hack of fout is, of hoe zeg je dat. Diegene die erachter zit die je probeert op te lichten, als die het goed doet dan kan het zijn dat je eromheen gaat omdat zij weten hoe de virusscanner scant, dus het is nooit 100%.
00:14:36
Zegert van der Linde: Nee, maar goed, 99% veilig is ook al best wat.
00:14:41
Esther Mieremet: Ja.
00:14:41
Zegert van der Linde: Als we het even terug vergelijken met het virus: als we een vaccin hebben dat 99% veilig is dan gaan we dansend de straat op met z'n allen.

00:14:49
Esther Mieremet: Ja, nee, klopt. En het is wel zo dat als je bijvoorbeeld iets wilt downloaden en je doet dat vanuit een appstore, dus de winkel van Microsoft of Apple of... Die zijn allemaal gecheckt, dus die zijn veilig. Ben je op een website en ga je vanaf een website iets downloaden dan is dat niet gecheckt via de appstore, dus de winkel van Microsoft, Google, Apple of wat dan ook. Dus dat is minder veilig dan wanneer je een app koopt die aangeboden wordt in de appstore.
00:14:50
Zegert van der Linde: Dus als je zeker wilt zijn dan neem je gewoon lekker die appstores.
00:15:29
Esther Mieremet: Ja. Die zijn allemaal gecheckt. En je moet ook aan voorwaarden voldoen als ontwikkelaar om daar iets op te krijgen. Dus als ik iets maak voor mensen en ik wil het daar kwijt, dan word ik ook gecheckt als maker, of ik betrouwbaar ben, maar ook of er geen rare dingen in de software zitten. Nogmaals: het is nooit 100% maar daar kan je wel gewoon vanuit gaan.
00:16:01
Zegert van der Linde: Het is natuurlijk ook zo met dit onderwerp dat als je alles continu gaat bijhouden, dat je dan heel zenuwachtig en bang gaat worden om dingen te gaan doen.
00:16:01
Esther Mieremet: Ja, en daarbij: ons huis beveiligen we heel goed met sleutels, maar er kan nog steeds een inbraak zijn, want het is nooit 100%. En dat geldt voor het internet natuurlijk ook.
00:16:14
Zegert van der Linde: Dat is precies hetzelfde. Als het dan toch misgaat dan kun je maar beter een back-up hebben. Heel kort: wat is een back-up?
00:16:23
Esther Mieremet: Een back-up is eigenlijk een... Je slaat dat wat je hebt op op een plek, waardoor als het weg is, dat je het terug kunt zetten. Dus het is eigenlijk een kopie van je systeem of van je documenten.
00:16:36
Zegert van der Linde: Ja, het kan ook zijn dat je ergens op een losse harde schijf al je documenten hebt voor het geval je laptop eens op de grond valt, zodat je je bestanden nog hebt. Het hoeft niet eens kwade wil te zijn.
00:16:51
Esther Mieremet: Nee, en het kan op twee manieren. Je kan het op een hard disk zetten, dus de schijf waar jij het net over had, maar je kan het ook gewoon in de cloud zetten, want de cloud is niet gerelateerd aan het apparaat dat je hebt. Dus dat betekent dat het er altijd is. En Microsoft of welke partij dan ook maakt dan ook een back-up, dus op het moment dat er iemand aan je gegevens zou kunnen, is er altijd nog een tweede versie.
00:16:59
Zegert van der Linde: Juist. Sommigen zeggen ook dat je meer dan één back-up moet maken. Bijvoorbeeld eentje in de cloud en eentje op een externe harde schijf. Is dat nog zo belangrijk?
00:17:34
Esther Mieremet: Ja... Dat moet niet. Het is ook een beetje een keuze van wat je belangrijk vindt hè. Ik kan me voorstellen dat je je foto's in een fotoalbum hebt in een kast. Als er dan brand is in huis dan heb je die foto's niet meer, dus je kiest nog een andere manier, je maakt namelijk foto's van je foto's en die zet je in de cloud. Dan heb je twee plekken, en dat vind ik een logisch iets. Terwijl een back-up van je computer op twee verschillende plekken... nou ja... Of het moeten foto's zijn want dat is iets wat lastig terug te halen is. Maar met het Microsoft systeem... Ja, dan loggen we in en dan downloaden we weer de nieuwe, weet je? Daar zit veel minder waarde aan.
00:18:20
Zegert van der Linde: Ja, dus je moet even goed nadenken hoe belangrijk iets is en of je het nog eens kan vervangen als het per ongeluk toch kwijtgeraakt?

00:18:29
Esther Mieremet: Ja, bijvoorbeeld je bankgegevens. De bank heeft jouw gegevens, dus je hoeft niet al je afschriften twee keer te gaan bewaren. Dat is niet nodig; je hebt ze.
00:18:37
Zegert van der Linde: Nee, dat deed je vroeger ook niet met je papieren afschriften. Dan had je ook gewoon één map en klaar, en niet drie.
00:18:43
Esther Mieremet: Nee, klopt.
00:18:44
Zegert van der Linde: Je hebt bepaalde software, programma's die dat kunnen doen, maar hebben Microsoft en Apple dat soort dingen ook al ingebouwd in hun systeem? Of moet je daar echt nog iets aparts voor hebben, voor een back-up?
00:18:55
Esther Mieremet: Een back-up moet je echt zelf handmatig doen, dus het op twee plekken zetten. Je kan inderdaad gewoon met een kabeltje een harde schijf koppelen aan je laptop of computer, en zeggen: deze documenten wil ik op die schijf. Dan heb je ze op allebei de plekken. En op het moment dat je het in de cloud hebt, een OneDrive of Google-map, die is al beveiligd en dubbel uitgevoerd, dus die hoef je niet twee keer te kopiëren. Daar heb je niet eens... Ja, je hebt er wel controle over, maar niet de fysieke controle want die staan dan op een server ergens in Amsterdam of...
00:19:35
Zegert van der Linde: ...ergens ver weg, een groot serverpark.
00:19:35
Esther Mieremet: ja.
00:19:35
Zegert van der Linde: Als ik een foto maak met mijn telefoon dan slaat ie de foto automatisch op op mijn telefoon, maar ook gelijk automatisch naar de cloud. Dus als er iets gebeurt met mijn telefoon dan kan ik nog altijd in de cloud die foto's zien.
00:19:50
Esther Mieremet: Ja. En als je telefoongeheugen niet zo groot is dan kan je de foto's ook gewoon wissen van je telefoon zodat je weer nieuwe foto's kunt maken en dat je niet een telefoon hoeft te kopen van - weet ik veel - 50 gigabyte, omdat je het ergens anders ook al opslaat.
00:20:03
Zegert van der Linde: Ja, en dan het onderwerp waar ik de podcast mee begon: een goed wachtwoord. Aan wat voor eisen moet nou een goed wachtwoord voldoen?
00:20:11
Esther Mieremet: Er zijn eigenlijk meerdere spelregels, en de eerste is: Het moet gewoon niet zo makkelijk te raden zijn.
00:20:15
Zegert van der Linde: Nee, dus wat ik in het begin opnoemde van: 123456, Welkom, Wachtwoord, dat is een beetje te gemakkelijk.
00:20:22
Esther Mieremet: Ja. Hallo123, Start123, Start1, de volgende maand Start2 en de volgende maand Start3. Je moet je voorstellen dat een oplichter dat niet zelf gaat intypen maar ze maken programma's om alle cijfers en alles erdoorheen te halen om te kijken: is dit er eentje die ik ken? Het wachtwoord zo lang mogelijk maken is eigenlijk al stap één: maak het zo lang mogelijk. Het is wel zo dat als je op een website bent dat ze soms bepaalde eisen hebben, zoals zorgen dat er een hoofdletter in zit. Dus dan moet je wel gewoon voldoen aan de eisen van die website waar je bent of app waar je toegang toe wilt. Dan kan je wel zelf dingen verzinnen maar dan moet je wel

gewoon aan hun eisen voldoen, wat gewoon een technisch iets is. En als je het helemaal zelf mag kiezen dan moet je het echt zo lang mogelijk maken, liefst een zin.

00:20:47

Zegert van der Linde: Een zin?

00:20:47

Esther Mieremet: Ja, want dat kan je ook relatief makkelijk onthouden. De logica van jouw zin snapt een computer niet hè, maar die snap jij wel. Als jij zegt: 'ikhebbijnadriejaarverkeringmetmijnliefde2021@', daar voel jij iets bij of daar heb jij een idee bij. Maar de computer kan al die woorden niet met elkaar koppelen dus die vindt het alleen maar heel veel tekens die hij moet... Hoe zeg je dat?

00:21:48

Zegert van der Linde: ... Moet uitvinden. En dan ook nog allemaal op de goeie plek. Die zin die jij zegt heeft misschien wel veertig letters, en die moet ie dan ook allemaal op de goeie plek zetten. Ik vind het soms ook wel gewoon irritant. Dan staat er weer zo'n wachtwoord en dan moet er een hoofdletter in, een kleine letter, een cijfer, een leesteken, en het moet twaalf karakaters lang zijn. Dan denk ik... (zucht): Oké, hier gaan we weer. Maar het is wel belangrijk?

00:22:20

Esther Mieremet: Het is belangrijk en wat misschien nog wel belangrijker is, is dat je eigenlijk bij alles een ander wachtwoord gebruikt. Je kan wel een heel moeilijk en lang wachtwoord hebben, maar als je dat overal gebruikt en ze hebben dat wachtwoord dan kunnen ze dus overal in. Dus je moet eigenljik voor elke app een ander wachtwoord hebben. Dat kan je niet onthouden, dus dan moet je een methode hebben of verzinnen hoe je dan zo'n wachtwoord kunt onthouden.

00:22:37

Zegert van der Linde: Ja, hoe dan?

00:22:53

Esther Mieremet: Nou, daar heb je wachtwoordmanagers voor, zoals dat heet. Dan moet je maar één wachtwoord onthouden en dan zet je in een soort kluis al je wachtwoorden.

00:23:05

Zegert van der Linde: Oh, oké. Dus dat is dan een appje ofzo?

00:23:12

Esther Mieremet: Ja.

00:23:12

Zegert van der Linde: Je logt dan in bij je app en dan staat daar je hele rij met wachtwoorden.

00:23:13

Esther Mieremet: Ja, en als je achter je computer zit en je zit in die kluis, dan kan je ook gewoon een wachtwoord kopiëren en plakken, zodat je ook niet alle tekens hoeft te onthouden. Je kan het bekijken, maar je kan het ook gewoon kopiëren en plakken.

00:23:33

Zegert van der Linde: En als er dan achter je rug iemand stiekem in de trein zit mee te kijken, dan ziet die het ook niet bijvoorbeeld?

00:23:33

Esther Mieremet: Nee.

00:23:43

Zegert van der Linde: Dan heb je al lekker die wachtwoorden, je hebt goeie, veilige wachtwoorden, en je hebt verschillende wachtwoorden die in je wachtwoordmanager zitten opgeslagen. En dan kom je steeds vaker tweestapsauthenticatie tegen. Wat is dat?

00:23:59

Esther Mieremet: Ja. Nou, dat is een beetje een lastig woord, maar het betekent eigenlijk dat er twee stappen zijn om

te komen in je applicatie of op de website of waar je ook wilt zijn. Dus twee stappen: je logt in, eerst door je A en dan door je B. En die twee stappen... één stap kan een oplichter misschien nog wel ontfutselen, maar twee stappen niet, en al helemaal niet als het op twee verschillende manieren gaat. Als voorbeeld: eerst moet je bijvoorbeeld met je duim een vingerafdrukscan maken op je smartphone of whatever, en het tweede is dan dat je je wachtwoord intypt. Dat zijn dus twee manieren om toegang tot iets te krijgen, als voorbeeld. Een ander voorbeeld is face-ID, bijvoorbeeld je iPhone die opent doordat je ernaar kijkt. Dat is dan nog een manier. En bij een bank krijg je bijvoorbeeld soms een sms-je en dan heb je ook twee stappen: een wachtwoord en een sms met een code en dan moet je die code op de website van de bank intoetsen.

00:25:12

Zegert van der Linde: Ja, en de kans dat ze dat allebei hebben...

00:25:16

Esther Mieremet: Die kans is echt heel klein. De banken zijn echt supergoed beveiligd, wat ook logisch is want het gaat over geld. Die zijn dus al begonnen daarmee, en eigenlijk zie je dat wat zij hebben bedacht of wat ze hebben gedaan... Eerst deden ze dat met van die 'identifiers' waar je je pasje in moest doen. Dat wordt nu steeds minder gekoppeld aan je pas maar steeds meer aan gewoon twee manieren.

00:25:37

Zegert van der Linde: En dus steeds vaker ook gewoon alleen aan je telefoon, die je dan moet gebruiken op één of andere manier.

00:25:37

Esther Mieremet: Ja.

00:25:41

Zegert van der Linde: Dan noem je ook wel iets interessants, want ik open mijn telefoon tegenwoordig ook met mijn gezicht. Dat was vroeger heel futuristisch maar nu gebeurt dat gewoon. Bedrijven krijgen daarmee dan ook toegang tot die informatie van jou. Ze krijgen mijn vingerafdruk of gezichtskenmerken. Kunnen ze daar iets mee? Behalve mijn telefoon openmaken?

00:26:07

Esther Mieremet: Nee, daar kunnen ze niks mee, en ze moeten ook vanwege regels van privacy zorgen dat dat niet gekoppeld wordt aan, en doorgegeven wordt, of überhaupt vastgelegd wordt in combinatie met jou. Dus het wordt wel vastgelegd omdat je anders niet erin komt, en daarna wordt er niks meer met die informatie gedaan, want dat wordt gescheiden.

00:26:27

Zegert van der Linde: Oké.

00:26:28

Esther Mieremet: Ja, dus de gegevens die je achterlaat - want dat is natuurlijk ook een interessant onderwerp om het over te hebben - dat is dit niet. Dit gaat echt over de toegang. Dit is de technische kant van het verhaal. Wat je met gegevens kunt doen als je op websites bent met cookies en dat soort dingen, dat is een hele andere discussie.

00:26:39

Zegert van der Linde: Een hele andere discussie, inderdaad. Ik zei daarnet al dat die gezichtsherkenning nog heel futuristisch was. Ik herinner me nog de eerste keer dat ik mijn telefoon opende met mijn vingerafdruk en dat ik dacht: wow. Dat is intussen al een klein beetje achterhaald, want je gezicht is de volgende. Hoe gaat dit verder?

00:27:05

Esther Mieremet: Ja, hele goeie vraag. Heel veel bedrijven, maar ook nieuwe bedrijven zijn natuurlijk sowieso aan het zoeken naar wat je nog meer kunt gebruiken en hoe je dat zo veilig mogelijk kunt doen. En dus een gezicht... Je merkt bijvoorbeeld dat als je je zonnebril op hebt dat je gezicht het niet doet.

00:27:25

Zegert van der Linde: Ja, of met een mondkapje op.

00:27:28

Esther Mieremet: Inderdaad. Maar je ziet ook dat... Ik had laatste een verkleedpartij en toen deed ie het wel, terwijl ik bijvoorbeeld grotere wimpers op had en iets op mijn neus. Dus je kan het nog veiliger maken, bijvoorbeeld door iets met je iris, met je oog te doen. Een duimafdruk is al uniek, maar men blijft dat wel verder ontwikkelen om te kijken of er nog meer is dat je kan gebruiken.

00:27:58

Zegert van der Linde: Wauw!

00:27:58

Esther Mieremet: Ja, het is wel interessant.

00:28:00

Zegert van der Linde: Ja, absoluut. Hartstikke mooi. Dank je wel voor deze uitleg, Esther.

00:28:04

Esther Mieremet: Oké, leuk!

00:28:07

Zegert van der Linde: Dit was de eerste aflevering van de SeniorWeb Podcast. U luisterde naar een gesprek met Esther Mieremet van veiliginternetten.nl. Wilt u meer tips en informatie over online veiligheid? Kijk dan op www.seniorweb.nl en klik op 'online veiligheid en privacy'. Wilt u de SeniorWeb Podcast volgen dan kan dat het makkelijkst via een podcast-app op uw telefoon. Kijk voor een uitleg op seniorweb.nl/podcast. Volgende week is er een nieuwe aflevering. Voor nu: bedankt voor het luisteren en tot de volgende keer.