Tijdschrift voor Communicatiewetenschap - jaargang 39 - nr. 2 2023

FR3EM

Lekkage

INTERVIEW CYBERHELDEN

CYBERCRIME RAPPORT

DATA DON'TS EN COOKIES

8 TIPS OM JE DATA TE BESCHERMEN

Redactieadres
Mycelium t.a.v. Freem
Postbus 9104
6500 HE Nijmegen
freem@mycelium.nu

Oplage
250 exemplaren

Hoofdredactie
Laura Haagmans

Eindredactie
Anouk van Bokhoven
Fleur Peters
Julie Rasing
Julia van Zoest
Laura Haagmans
Samantha Vanc

Beeldredactie
Anouk van Bokhoven
Floor Crousen
Julie van Kerkhoff
Lieke Spee
Me'Shell Provence

Tekstredactie
Eva Gerritsen
Eva Slot
Fleur Peters
Iza Versantvoort
Julia van Zoest
Julie Rasing
Lotte Meeuse
Samantha van Cadsand

Speciale bijdrage van
Myceliumbestuur
OLC

Copyright
Het is niet toegestaan zonder voorafgaande en uitdrukkelijke toestemming van de hoofdredacteur door Freem gepubliceerde artikelen geheel of gedeeltelijk over te nemen, te publiceren of anderzijds openbaar te maken of te verveelvoudigen.

Advertenties
www.texperts.nl
Rabobank

Social Media
FreemCW
FreemCW

VOORWOORD

Drup, drup, drup, lekkage!

The big world wide web is voor mij maar een vaag concept. Ik vraag me dan ook regelmatig af wat er eigenlijk allemaal gebeurt met mijn data, mijn gegevens, mijn geheimen in deze digitale massa. Moet ik me bijvoorbeeld zorgen maken wanneer er een **datalek** is bij Facebook? Of is het grootste geheim dat Facebook van mij heeft, dat ik van kattenvideo's houd? Is mijn data wel veilig online?

En in de 'echte' wereld, deel ik ook van alles met Jan en alleman. Maar een beetje privacy waardeer wel. Voor *celebs* is **privacy** in dit digitale tijdperk haast onmogelijk. Een keer gespot worden met een *chickie* en de volgende dag staat heel **Tiktok** er vol mee.

Het lijkt me vre-se-lijk! Hoe houd je iets geheim, met alle roddel kanalen die je continu in de gaten houden?

In deze editie staat omgaan met **data, privacy en geheimen** centraal.

We bespreken cybercrime in de *reportage*, en geven jullie tips hoe je je data beter kan beschermen in *How to - protect your data*. Ook spreken we Ronald Prins in het *interview* over zijn podcast met echte Cyberhelden. En besteden we aandacht aan de *Luisterlijn*, zodat jij altijd een plek hebt waar jij je geheimen veilig kwijt kan!

Na deze editie weet jij hoe je een **lekkage** kan voorkomen! Tenminste een datalek, of geheimen-lek.
(Succes niet gegarandeerd)

Laura Haagmans
Hoofdredactrice 2022-2023

INHOUDSOPGAVE

Interview: cyberheld Ronald Prins	4
Studenten VS Docenten	7
Cybercrime rapport	8
Pic(k) your fave	13
Mycelium Outside	14
Column: bereikbaarheid	16
Storing: diner in het OV.	17
Luisterlijn	18
Trends	20
Day in the life of	22
Quiz	23
Data don'ts	24
How to... protect your data	26
What do the socials say?	28
OLC update	30
Nawoord	31

INTERVIEW MET CYBERHELD: RONALD PRINS

TEKST IZA VERSANTVOORT & FLEUR PETERS
BEELD JULIE VAN KERKHOFF

Cybersecurity: de activiteit en het inrichten van een computer om deze te beschermen tegen bedreigingen als virusaanvallen en spam. Dit is iets wat in de huidige maatschappij steeds belangrijker wordt en waar veel bedrijven zich mee bezighouden. Wij gingen in gesprek met Ronald Prins, de man die in zijn podcast "Cyberhelden" met de 52 grootste securityhelden in gesprek ging over hun visie op cybersecurity in Nederland.

Wat houdt Cyberhelden de podcast in?
"De podcast is inmiddels gestopt, maar ik heb die podcast gemaakt omdat ik het leuk vind: ik ken ontzettend veel mensen in het cyberdomein. Ik denk dat de buitenwereld niet zo bekend is met deze mensen dus ik vond het leuk om er een aantal in de spotlight te zetten. Aangezien ik deze mensen al regelmatig spreek dacht ik: wat als ik het nou opneem? Misschien vinden andere mensen het dan wel interessant om naar te luisteren.

Hoe kwam u op het idee om aan de podcast te beginnen?
Ik heb altijd het idee gehad dat ik mijn gedachten wil uitdragen, en toen dacht ik: ik kan het wel zelf steeds zeggen, maar ik kan ook mensen interviewen en tijdens het bespreken van bepaalde thema's het gesprek misschien wel een bepaalde richting in sturen. Zo wilde ik de awareness rond cybersecurity naar boven halen. Ik ben ook in gesprek gegaan met de baas van de AIVD omdat ik vind dat de Nederlandse overheid te weinig doet aan het tegengaan van economische spionage door andere landen. Dat zijn dingen die ik mooi kan aankaarten tijdens het maken van de podcast. Ik merkte ook dat veel journalisten naar mijn podcast luisterde, BNR heeft een hele lijst van mijn gasten na het opnemen van de podcast gevraagd om ook langs te komen.
Op een gegeven moment had ik 52 afleveringen gemaakt. Ik moest al steeds dieper gaan graven voor mensen die nog leuk zouden zijn, ik was een beetje door de echte **cyberhelden** heen, dus toen kon ik ermee stoppen.

Hoe komt het dat u de cyberhelden in het dagelijks leven al kende?
Dat kom vanwege mijn werk. Ik ben niet executief. wat betekent dat ik eigenlijk niks doe en alleen maar investeerder ben en in hele grote lijnen richting geef. Maar in het algemeen is wat het bedrijf doet het helpen van andere bedrijven in het tegengaan van digitale spionage. Waar we ons nu mee bezighouden zijn bedrijven die veel in Nederland zijn, vaak familiebedrijven, die mooie uitvindingen doen. Dat gaat van technologie tot funderingen voor windmolenparken. We proberen buitenlandse spionage in deze bedrijven tegen te gaan. Ik ben persoonlijk in het bedrijf veel met de media bezig en geef dan ook vaker interviews.

We zagen dat u wiskunde gestudeerd heeft, hoe heeft u de overstap van wiskunde naar de cyberwereld gemaakt?
Ik ben wiskunde gaan doen omdat ik dat kon. Het is uiteindelijk ook de makkelijkste studie die er is. Één van de onderdelen van wiskunde is geheimschriften in het vakgebied cryptografie. Ik ben in dit vakgebied afgestudeerd en vervolgens bij het gerechtelijk laboratorium gaan werken om de geheimen te kraken van

CYBERHELDEN DE PODCAST

criminelen. Uiteindelijk bleek dat deze wereld van informatie beschermen en informatie geheim proberen te houden veel breder is geworden. Dit is wat we nu cybersecurity noemen.

Wij merken heel erg dat studenten onder ons niet zo bezig zijn met het beveiligen van hun data. We weten niet of u zich ook bezighoudt met persoonlijke databeveiliging, maar denkt u dat we hier meer mee bezig zouden moeten zijn?
Ik denk dat we daar met zijn allen een beetje **spastisch** over aan het doen zijn, dat we alles moeten beschermen. Ik merk wel dat de meeste mensen eigenlijk al goede afwegingen kunnen maken. Het appen van je pincode naar andere mensen is natuurlijk niet slim, die moet je gewoon geheimhouden. Iets waar iedereen heel hard voor zit te waarschuwen zijn openbare wifinetwerken, maar eigenlijk is alles tegenwoordig gewoon altijd standaard versleuteld. Dus als jij ergens in een cafétje je laptop opent en besluit je mail te gaan lezen, dan kan ik dat niet afluisteren, dus die beveiliging is echt goed. Waar we bang voor zijn, is dat data lekt en dat bestanden gestolen worden, bijvoorbeeld een database bij LinkedIn. Het enige wat mensen dan te zien krijgen is wie je contacten zijn, dus ik ben er zelf eigenlijk heel laks in. Ik heb al mijn wachtwoorden in een passwordmanager gestopt. Dat is zoiets als je sleutelhanger die in de iCloud alles bewaart. Nu blijkt het dus dat zij laatst een storing hebben gehad, waarbij ik bewust niet alles heb veranderd, omdat ik voor alle belangrijke dingen nog een tweede factor heb die mijn gegevens beveiligd. Terwijl ik dus best wel wat geheimpjes heb, ga ik er alsnog redelijk relaxed mee om. Ik vind dat de media hier soms ontzettend **spastisch** over doet als er bijvoorbeeld een lek bij de gemeente of politie is geweest. Vaak zijn dit alleen maar NAW-gegevens die vrijgegeven worden en die stonden een paar jaar geleden ook nog gewoon in het telefoonboek. Er worden vaak allerlei scenario's verspreid over hoe criminelen dat zouden misbruiken, over hoe je dan spam zou kunnen krijgen of vision mail, maar in de praktijk valt dat heel erg mee.

Dus eigenlijk moeten alleen degenen waarmee u zich bezighoudt, de grote bedrijven, zich erg zorgen maken over het beschermen van hun data?
Ja, ik denk het wel. Daar vindt ook echt gerichte spionage plaats. Maar in principe hebben privépersonen ook gewoon recht op privacy. Iedereen kijkt wel eens een gek filmpje. Ik merk aan de andere kant wel dat de meeste mensen zeggen: "Ja ik kijk porno, maar dat doet bijna iedereen, dus dat zie je dan maar een keer". Vooral oudere mensen vinden het heel moeilijk, maar de jongere generatie vindt het allemaal wel normaal.

Heeft u zelf nog een favoriete aflevering uit de podcastserie die u zelf heeft gemaakt?
Nou, ik heb er eentje en hier heb ik ook een dubbele aflevering over gemaakt met Peter Koop. Dit gaat over spionage en Edward Snowden, ik weet niet of jullie hem kennen. Edward noemt zichzelf de **klokkenluider,** waarvan ik denk dat hij gewoon een verrader is, en die allerlei geheimen aan de Russen heeft verteld. Peter Koop heeft zijn leven eraan gewijd alles te weten te komen over deze praktijken. Ik vond dit zo fascinerend dat ik tijdens de opnames heb besloten om er een dubbele aflevering van te maken van in totaal een uur lang."

STUDENTEN VS DOCENTEN

DEZE EDITIE: EVELIEN VS HILDE

Hoe kijken studenten en docenten tegen een open Instagram account aan? Houden docenten stiekem van online juice? Worden studenten flink gehackt? We vroegen het docent Evelien Heijselaar en student Hilde Scholten.

TEKST JULIE RASING
BEELD FLOOR CROUSEN

Zijn je sociale-media-accounts open of gesloten en heb je hier bewust voor gekozen?
Evelien: "Beetje van beide. Volgens mij kan je me wel vinden op sociale media, maar sommige informatie is verborgen totdat we 'vrienden' zijn. Ik heb hier bewust voor gekozen en probeer regelmatig in de *security settings* te kijken of het nog *up-to-date* is, omdat je niet altijd weet wanneer ze weer iets hebben aangepast. Grote kans dat jullie mij nu gaan zoeken, dus ik hoop dat alles nog klopt!"

Hilde: "Ik heb een gesloten Instagramaccount en ik accepteer ook alleen maar mensen die ik (vaag) ken. Ik vind het niet nodig dat iedereen kan zien wat ik doe of waar ik op vakantie ben. Ik wil graag een beetje controle houden. Ik vind Instagram een leuke app om dingen op te posten en om mijn creativiteit op te uiten, maar ik heb geen ambities als *influencer*. Dus veel volgers zijn niet relevant."

Ben jij wel eens gehackt of ken je iemand in je omgeving bij wie dit is overkomen?
Evelien: "Ja, ik ben ooit wel eens gehackt door een ex die selectieve berichten naar vrienden stuurde om ze tegen mij te keren. Leuk moment in mijn leven. Ik weet nog steeds niet hoe die het heeft gedaan. Ik denk toch dat ik eens mijn laptop niet vergrendeld had en dat hij toen van alles heeft gelezen."

Hilde: "Lang geleden is mijn Instagram gehackt. Toen stond er ineens een advertentie op mijn feed voor een Nike-schoen, die ik er nooit zelf op had gezet. Daarna was mijn account geblokkeerd. Ik had zo'n schimmige app waarmee je kon zien wie je had ontvolgd, ik denk dat het daardoor kwam. Ik had geen zin om een nieuw account aan te maken en heb toen vier jaar lang geen Instagram gehad. Het beviel me prima. maar omdat ik toch te veel FOMO had, heb ik de app weer geïnstalleerd."

Volg je roddelprogramma's, roddelkanalen of roddelaccounts en waarom?
Evelien: "Ik zit vaak op 9gag, telt dat? Het is meestal roddel. Ik vind het leuk om bij te houden wat de massa vindt van wat er gebeurt in de wereld. Heel vaak merk je dat jij en je vrienden toch in de minderheid zitten (of soms niet) en dat is belangrijk om in acht te houden."

Hilde: "Nee, ik volg geen *juicechannels*. Wel betrap ik mezelf erop dat ik op telefoons van vriendinnen toch even bij Lifeof Yvonne ga kijken. Zij heeft een gesloten profiel waardoor het een beetje 'alles of niks' is. Maar op een andere telefoon kan ik dan toch even kijken wat er speelt. Ik volg haar zelf niet, omdat ik *juicechannels* geen podium wil geven en omdat ik het niet eens ben met de manier waarop informatie naar buiten wordt gebracht. Ik hou mezelf ook voor dat ik het niet interessant vind, maar dat laatste is dus eigenlijk niet waar."

CYBERCRIME

RAPPORT

TEKST JULIE RASING & EVA SLOT
BEELD LIEKE SPEE

Hoeveel nepverzoeken, berichtjes van banken en linkjes naar zogenaamde winacties heb jij al eens ontvangen? Waarschijnlijk al zoveel dat het niet eens meer op één hand te tellen is. De afgelopen jaren is meer dan de helft van alle Nederlanders namelijk wel eens geconfronteerd met cybercrime. Hierdoor voelen veel mensen zich tegenwoordig online minder veilig dan op straat. Cybercrime is immers niet altijd direct herkenbaar en zorgt ervoor dat criminaliteit je eigen telefoon en computer binnendringt.

Cybercrime is de verzamelnaam voor alle criminele activiteiten die zijn gericht op een computer, een netwerk of een netwerkapparaat. Bij dit type criminaliteit wordt dus een ICT-systeem gebruikt als middel om het delict te plegen en is een ICT-systeem het **doelwit** van het delict. De meeste cybercriminaliteit wordt gepleegd door cybercriminelen of door hackers en heeft het doel om geld te verdienen. Toch kan cybercrime ook gericht zijn op het beschadigen van computers of netwerken om andere redenen dan alleen geld. Ook vallen hackers vaak bedrijven aan met het doel om gevoelige informatie te verkrijgen. Die gegevens worden vervolgens **doorverkocht** of gebruikt om iemand af te persen.

Cybercrime komt voor in meerdere vormen. Eén van de meest bekende en voorkomende vorm is **phishing**, oftewel het 'vissen' van criminelen naar informatie via WhatsApp, SMS of e-mail. De afzender van deze berichten doet zich voor als iemand anders, vaak iemand die je persoonlijk kent, en zet je onder druk om op een link te klikken of geld over te maken. Klik dus nooit op links in berichten van onbekenden, want daarmee kan je schadelijke software (malware) installeren.

Heb je toch op een schadelijke link geklikt? Dan loop je de kans om 'gegijzeld' te worden door **ransomware.** Dit is malware die je systeem, data of netwerk op slot zet waardoor je niet meer kan werken met je systeem of bestanden. De sleutel tot je bestanden krijg je vervolgens alleen terug in ruil voor losgeld. In 2021 was RTL Nederland slachtoffer van een ransomware-aanval. De inlog-

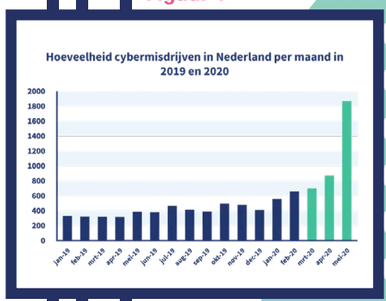
gegevens van een werknemer waren achterhaald en door de afwezigheid van een dubbele beveiliging (zoals een tweestapsverificatie) kregen de aanvallers direct verregaande toegang op het netwerk van RTL. Vervolgens werd een aantal computers, servers en systemen gegijzeld en deels ontoegankelijk gemaakt. RTL heeft uiteindelijk 8500 euro aan de aanvallers betaald.

Een andere veelvoorkomende vorm van cybercrime is een **DDoS-aanval,** oftewel een Distributed Denial of Service-aanval. Hierbij versturen cybercriminelen zoveel dataverkeer naar een server, website of app dat die voor bezoekers onbereikbaar wordt. Vaak zijn deze DDoS-aanvallen een afleidingsmanoeuvre: wanneer er wordt gezocht naar een oplossing, proberen criminelen data te stelen.

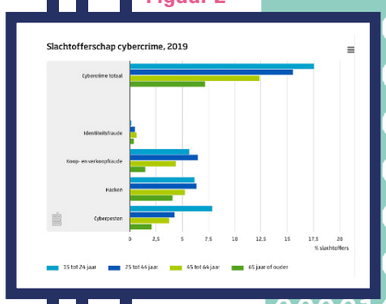
Sinds 2012 is het aantal mensen dat in Nederland slachtoffer zijn geworden van cybercrime toegenomen met 22%. Vooral de laatste jaren neemt cybercrime enorm toe. De vorm van cybercrime die de afgelopen tijd het meest is toegenomen is **aankoopfraude.** Je maakt geld over naar een persoon of bedrijf, zonder dat je de dienst of het product ontvangt waarvoor is betaald. Het percentage mensen dat slachtoffer is van hackers blijft vrij stabiel, en het aantal slachtoffers van **identiteitsfraude** neemt de laatste jaren af.
In 2021 was 17% van de Nederlandse bevolking van 15 jaar en ouder slachtoffer van een of meer online delicten. Jongeren zijn vaker slachtoffer dan ouderen: in 2021 was 20% van de 15- tot 25-jarigen slachtoffer van cybercrime, terwijl 12% van de 65-plussers hiervan slachtoffer was. Voor meer statistiek van cybercrime, zie figuur 1 en figuur 2.

Hoe zit dit op andere plekken in de wereld? Hoe doet Nederland het in vergelijking met andere landen? Onze zuiderburen, België, staan op de derde plek van de **National Cyber Security Index (NCSI)** in januari 2023. De NCSI is een wereldwijde live index, die de paraatheid van landen meet om cyberincidenten te beheersen. Op de eerste plaats staat Griekenland, gevolgd

Figuur 1



Figuur 2



door Litouwen. Nederland staat op plaats 18. In 2022 had het Verenigd Koninkrijk de meeste slachtoffers van cybercrime, gevolgd door de Verenigde Staten.

De gevolgen van cybercrime zijn heel verschillend. Het kan je veel geld kosten als cybercriminelen op jouw naam een lening aanvragen. Ook kunnen alle soorten cybercrime leiden tot een **datalek.** Daarnaast loop je risico op identiteitsfraude, en dit kan emotioneel heel erg belastend zijn. Zo kunnen de criminelen gevoelige gegevens van klanten bij een bedrijf in handen krijgen. Naast bedrijven worden ook organisaties slachtoffer van cybercrime, zoals de HAN (Hogeschool Arnhem Nijmegen). In 2021 zijn zij slachtoffer geworden van een hacker en daarbij ook honderdduizenden (oud)studenten van wie persoonlijke gegevens in de handen van de hacker zijn gevallen. Kortom: probeer cybercrime te **voorkomen!**

Verdiende loon of niet, cybercriminelen lopen kans op flinke straffen. In Nederland kunnen criminelen die computergegevens vernielen een gevangenisstraf van maximaal 2 jaar krijgen. Het ontoegankelijk maken van computersystemen kan je ook maximaal 2 jaar in de gevangenis doen belanden. **Computercriminelen** die strafbare feiten plegen met een botnet, computers waarop malware is geïnstalleerd, kunnen maximaal 3 jaar gevangenisstraf krijgen. Breng je als cybercrimineel ernstige schade toe, zoals een aanval op een overheidsnetwerk of energiecentrale? Reken dan maar op een maximale gevangenisstraf van 5 jaar.

Bronnen:

- https://www.om.nl/onderwerpen/cybercrime
- https://longreads.cbs.nl/nederland-in-cijfers-2020/hoe-zit-het-met-cybercrime/#:~:text=Jongeren%20zijn%20vaker%20dan%20ouderen,(7%2C9%20procent).
- https://veiliginternetten.nl/thema/cybercrime-en-incidenten/phishing-corona/wat-een-phishingmail/
- https://www.rijksoverheid.nl/onderwerpen/cybercrime-en-cybersecurity/cybercriminaliteit-bestrijden
- https://ncsi.ega.ee/ncsi-index/
- https://www.rtlnieuws.nl/nieuws/nederland/artikel/5255983/rtl-nederland-ransomware-aanval-cybercriminelen-losgeld
- https://www.han.nl/nieuws/2021/10/han-rondt-onderzoek-datalek-af-en-informeert-mogelijk-getroffenen/
- https://www.vpngids.nl/veilig-internet/cybercrime/cybercrime-statistieken-nederland/

Als je graag nóg meer over cybercrime te weten wil komen, zijn er op Netflix en Videoland genoeg interessante documentaires over dit onderwerp te bekijken. We hebben daarom de leukste docu's voor je op een rijtje gezet!

Ik Weet Je Wachtwoord (Videoland)
In deze documentaire duikt cybercrime journalist Daniël Verlaan in de wereld van ransomware-criminelen en laat hij je zien hoe makkelijk het voor hackers is om op afstand andermans leven te ontregelen. Daniël neemt je mee in de schimmige wereld van **online criminaliteit,** legt gevaren bloot, spreekt slachtoffers en verkent de wereld van de daders. Hij doet dit niet om mensen bang te maken, maar om ze ervan bewust te maken dat onze groeiende onafhankelijkheid van het internet gevaren met zich meebrengt waar iedereen vroeg of laat mee te maken kan krijgen. Heb je na het zien van deze afleveringen nog geen genoeg van het onderwerp cybercrime? Dan kan je ook nog de gelijknamige podcast luisteren, of het boek lezen.

The Tinder Swindler (Netflix)
Iedereen weet dat daten via een datingapp niet zonder ***catfish*-risico** is, maar deze documentaire laat zien dat zo'n date nog veel ergere gevolgen kan hebben. In deze docu wordt het verhaal van de Israëlische Shimon Hayut verteld, die vrouwen via Tinder voor miljoenen dollar op wist te lichten. Drie slachtoffers van Shimon komen in deze documentaire aan het woord en vertellen hoe hij zich voordeed als iemand anders. Hij noemde zichzelf bijvoorbeeld Simon Leviev, **oftewel Prince of Diamonds,** en deed alsof hij de zoon was van een rijke zakenman. Hij nam de vrouwen mee in privéjets en naar vijfsterrenhotels, maar al gauw wordt duidelijk dat er een addertje onder het gras zit. We gaan natuurlijk niet *spoilen* hoe het verhaal afloopt, dus dat zul je zelf op Netflix moeten bekijken!

The Great Hack (Netflix)
In deze documentaire ontdek je hoe het databedrijf Cambridge Analytica tijdens de presidentsverkiezingen en tijdens de Brexit-stemming in 2016 het symbool werd voor de duistere kant van social media. Het databedrijf (dat nu niet meer bestaat) gebruikte **persoonsgegevens** van Facebook-gebruikers, zonder hun medeweten of toestemming, om ze te categoriseren. Door deze persoonsgegevens te delen met klanten, kon Cambridge Analytica kennis delen over hoe deze Facebook-gebruikers het beste konden worden bereikt. Het databedrijf zou samen hebben gewerkt met Donald Trump aan zijn presidentiële campagne in 2016 en heeft kiezers dus mogelijk onbewust aangestuurd om op hem te **stemmen.** Ook wordt het databedrijf geassocieerd met andere politieke campagnes over de hele wereld. Eigenlijk zou iedereen met een social media-account deze docu zeker gezien moeten hebben!

Ze Weten Alles Van Je (Videoland)
In augustus 2018 verdwijnt de Nederlandse cyberexpert Arjen Kamphuis tijdens een vakantie in Noorwegen. Zijn kajak werd gevonden in een fjord, maar een paar dagen later maakte het mobieltje van Kamphuis nog contact met het netwerk in het zuiden van Scandinavië. Kortom: de verdwijning van Arjen Kamphuis is tot op de dag van vandaag één groot **mysterie.** Deze serie is eigenlijk een mix van nagespeelde scènes en documentaire. De vrienden van Arjen Kamphuis worden geïnterviewd, maar we zien ook actrice Charlie Chan Dagelet afreizen naar Noorwegen om antwoorden te vinden. Hierbij interviewt zij echte personen die iets te maken kunnen hebben met het onderzoek naar Arjen Kamphuis. Een erg spannende serie om te kijken dus!

Het láátste
wat ik
wil worden
is **tekstschrijver**
is met afstand
het leukste
communicatieberoep

Ben je geïnteresseerd in communicatie, tekst en gedragspsychologie? Dan zou je toch eens moeten overwegen om tekstschrijver te worden. Kijk maar eens op de website van Texperts. Dan begrijp je meteen dat tekstschrijven met afstand het leukste communicatieberoep is. **Én dat je zojuist hebt gehapt op de 'Disrupt-then-reframe'-techniek...**

www.texperts.nl

PIC(K) YOUR FAVE

Dagelijks komen we cookies tegen. Zonder er echt over na te denken zullen de meesten van ons deze gewoon accepteren. Elke keer dat jij cookies accepteert vormt zich een hele database aan gegevens over jou. Een belangrijke, en misschien wel lekkere, vraag die wij aan vier Myceliumleden stelden: Wat is jouw favoriete koekje en waarom?

TEKST LOTTE MEEUSE
BEELD JULIE VAN KERKHOFF

Denise van der Poel
Tweedejaars

Mijn favoriete koekje is een gangmaker. Naast mijn ongelofelijke verslaving aan chocolade (al helemaal in combinatie met die vulling, zo enorm lekker) is mijn vriendengroep van thuis thuis vernoemd naar deze heerlijke koek. Het koekje is gewoon enorm lekker, maar het herinnert me dus ook aan mijn lieve vrienden uit Arnhem.

Tess Wiedemeijer
Eerstejaars

Mijn lievelingskoekje is de American cookie witte chocolade macadamia. Als ik tussen de colleges door zin heb in iets zoets, haal ik deze vaak bij de Spar. De textuur van het koekje samen met de witte chocolade is echt een heerlijke combinatie.

Hannah Mannaerts
Vijfdejaars

Mijn favoriete koekje is een eierkoek! Misschien niet standaard zoals een bastogne of een krakeling, maar wel erg lekker. Iedereen die mij een beetje kent weet ook dat ze me altijd kunnen porren voor een eierkoek, groot of klein. Eigenlijk heb ik altijd wel eierkoeken in huis, vroeger vond mijn moeder het handig als we lange ritten in de auto maakten om er wat mee te nemen. Doordat we ze thuis zo vaak hadden, heb ik dit onbewust een beetje meegenomen in mijn eigen leven haha! Als ik een eierkoek eet krijg ik altijd weer een beetje het gevoel van vroeger, plus ze zijn gewoon erg lekker, dus daarom is het mijn favoriete koekje!

Mirthe Raats
Tweedejaars

Mijn favoriete koekjes zijn echt by far koekjes met kaneel! Kiezen tussen al die opties is heel lastig, maar deze Zweedse cinnamon rolls zijn voor mij de absolute topper. Je moet er een rondje (veel te drukke) IKEA voor over hebben, maar dat zijn ze zéker waard...

MYCELIUM OUTSIDE

TEKST JULIA VAN ZOEST & LOTTE MEEUSE
BEELD ME'SHELL PROVENCE

Een paar weken geleden vertrok een aantal CW-studenten naar het buitenland. In deze editie van de Freem vertellen zij over hun ervaringen in het buitenland. Hoe ziet hun leven er nu uit? Waarin verschillen Zweden, België, Denemarken en Portugal van Nederland? Tijd voor Mycelium Outside!

Naam: Liv Sijben
Waar: Göteborg, Zweden

Welke vakken volg je daar?
"Ik volg een minor in Genderwetenschappen aan de universiteit van Göteborg. Ik volg vier vakken die verspreid zijn over 1 semester. Mijn eerste vak is nu bijna afgelopen, Scandinavian Film and Media Culture. Voor dit vak had ik elke week één lecture en één film screening, waarin we elke keer een andere film keken. Geen vervelende les dus!

Hoe vermaak je je buiten de universiteit om?
De stad is heel groot en omringd met mooie natuur, er is genoeg te ontdekken! Vooral in het weekend proberen we de omgeving te verkennen door wandelingen te maken. En doordeweeks maken we goed gebruik van het concept Afterwork. Dit is een actie van pubs in de stad om mensen na hun werk naar binnen te lokken, waarbij je bij aankoop van een drankje gratis eten krijgt. Dit kan bestaan uit een heel buffet, maar ook uit taco's of pizza!

Wat mis je het meest aan Nederland?
Het brood, de kaas en de wijn, hahaha! Wijn is ontzettend duur hier en je kunt het alleen kopen in speciale winkels. Een glaasje wijn bij het avondeten zit er dus helaas niet in hier. En natuurlijk mis ik mijn vrienden en familie, maar ik vermaak me hier goed.

Waarover in dit land verbaas je je het meeste?
Het vertrouwen dat mensen hier in elkaar hebben. Zo hoef je bijvoorbeeld niet in te checken voor het openbaar vervoer: ze vertrouwen er gewoon op dat je een kaartje hebt gekocht. Zo nu en dan worden mensen gecontroleerd, maar ikzelf ben nog nooit gecontroleerd. Waar ik me nog meer over verbaasde is dat je in een café of bar vaak zelf het bedrag moet intoetsen voordat je gaat betalen. Dit doen ze, zodat je een fooi kan geven."

Naam: Lotte Bosscher
Waar: Roskilde, Denemarken

Welke vakken volg je daar?
"Ik volg hier een semester Social Psychology of Everyday Life. Het is anders dan ik verwacht had. Tot nu toe is het erg filosofisch en ik hoop dat daar nog verandering in komt. Verder hebben we een halfjaarlijks project.

Hoe vermaak je je buiten de universiteit om?
Ik heb hier een vriendengroep waarmee we al vele dingen hebben gedaan: een feestje in de RUCbar (vergelijkbaar met ons CultuurCafé), een spelletje in iemands dorm (op mijn verzoek vaak ezelen) en een internationaal feest in een ander studentengebouw. Daarnaast is Kopenhagen om de hoek en is er in de stad genoeg vermaak voor ons. Ook is er een mega leuk café in Roskilde, waar internationale jongeren en vrijwilligers samen het café runnen. Hier ben ik er inmiddels één van, zo doe ik hier ook nog eens horeca-ervaring op!

Wat mis je het meest aan Nederland?
Ik mis de gebakken aardappeltjes in een zak die je zo kan opbakken, en een extra belegen kaas. Daarnaast mis ik de euro, dat was gewoon een stuk gemakkelijker. Natuurlijk mis ik mijn familie ook, het is toch wel jammer dat ik niet binnen 2 uurtjes thuis kan zijn om op de koffie te komen in de Achterhoek.

Waarover verbaas je je in dit land het meest?
Denemarken was toch plat? Ik schaam me ervoor hoe erg ik buiten adem ben als ik vijftien minuutjes naar de Lidl of Aldi fiets. Er zijn hier toch zeker wel heuvels en veel wind. Toch ben ik allang blij dat ik een fiets heb kunnen regelen. Daarnaast verbaas ik me erover hoe gesloten Denen zijn. In mijn huis hebben we dan ook huisavond zonder de vier Denen. Al zijn ze wel heel behulpzaam en praten ze in de les allemaal Engels."

Naam: Julie van Kerkhoff
Waar: Antwerpen, België

Welke vakken volg je daar?
"Ik volg voor mijn minor zowel Vlaamse vakken als Engelse vakken binnen de communicatiewetenschap, zoals Nieuws & journalistiek en Interpersonal and Intercultural Communication.

Hoe vermaak je je buiten de universiteit om?
Mijn rooster is eigenlijk heel chill, doordat ik elke maandag en vrijdag vrij ben. Hierdoor heb ik al heel vroeg weekend en kan ik bijvoorbeeld voor een lang weekend naar huis of met vrienden Belgische steden ontdekken. Daarnaast heb ik al wat weekenden gepland waarin vriendinnen van thuis langskomen. Naast alle tripjes wil ook heel graag gaan werken in een leuk koffietentje in Antwerpen, zodat ik ook nog wat geld kan bijverdienen :).

Wat mis je het meest aan Nederland?
Heel cliché, maar toch wel mijn familie en vrienden. Ondanks dat ik niet heel ver weg ben en naar huis kan gaan wanneer ik wil, mis ik ze toch. Je bent heel erg op jezelf aangewezen, wat aan de ene kant heel goed is, maar aan de andere kant soms best eenzaam. Gelukkig willen ze me vaak genoeg komen opzoeken!

Waarover in dit land verbaas je je het meeste?
In België is het heel gebruikelijk om na een college 'op café te gaan', ook al is het 11 uur 's ochtends. Hier drinken ze dan geen koffie, maar gaan ze gelijk aan het bier. Een ander punt waarover ik me verbaas is de tijd waarop colleges beginnen. Ik begin namelijk pas om 09:30, heel fijn en veel beter dan 08:30!"

Naam: Elyse Kruit
Waar: Porto, Portugal

Welke vakken volg je daar?
"Ik volg momenteel drie vakken, aangezien ik mijn bachelor al heb gehaald en dus de punten niet nodig heb. Dit is Portugees voor beginners, Public Relations and Assessorship of Communication en Minorities: Gender, Sexualities and Ethnicities. Portugees wilde ik echt heel graag leren, en de andere twee vakken heb ik uiteindelijk na aankomst gekozen, met name omdat deze wel in het Engels worden gegeven. Aardig wat vakken bleken toen ik hier aankwam toch ineens niet in het Engels gegeven te worden.

Hoe vermaak je je buiten de universiteit om?
Hier in Porto is echt zat te doen. De stad is prachtig en ik kan me uren vermaken met rondstruinen door de prachtige straatjes en parkjes. Ik ben al wezen surfen en heb heerlijke picknicks op het strand gehad. Daarnaast worden er veel activiteit georganiseerd door evenementenbureaus voor internationals. Het is eerder de vraag hoe je je niet vermaakt, dan hoe je je wel vermaakt!

Wat mis je het meest aan Nederland?
Als ik eerlijk ben mis ik op dit moment nog niet zoveel. Ik ben hier pas twee weken en ben gewoon echt volop aan het genieten. Tuurlijk mis ik mijn lieve vrienden en het prachtige Mycelium, maar ik heb hier ook al heel veel lieve mensen ontmoet en daarbij genoeg afleiding. Voorlopig wil ik echt nog niet terug!

Waarover in dit land verbaas je je het meeste?
Hoe verschrikkelijk aardig alle Portugezen zijn. Ik had nooit verwacht dat ik me zo snel thuis zou voelen, maar dat komt echt door de stad en de mensen. En, ook noemenswaardig, iedereen hier betaalt apart! Ze vinden het dan ook geen probleem dat je, wanneer je met tien personen hebt gegeten, de rekening wilt splitten. Dat hoeven wij in Nederland niet te proberen ;)."

EEN ODE AAN BEREIKBAAR ZIJN

TEKST IZA VERSANTVOORT
BEELD JULIE VAN KERKHOFF

"Waar ben je?" Geen avondje uit met mijn vriendinnen is compleet zonder dit appje. Ik nam dit feit altijd voor lief tot afgelopen carnaval, toen door de bizarre drukte in Den Bosch er in de Korte Put geen bereik was. Hier bleek maar weer: soms weet je pas wat je hebt als je het even moet missen.

Zonder bereik in een **overvolle kroeg** bleek het een hele opgave om mijn vriendinnen terug te vinden zonder het gemak van telefonisch bereik. Belangrijk hierbij te vermelden is dat er al 22:00u op de klok stond en wij als echte Brabantse meisjes al vanaf 14:00u onszelf aan het vermaken waren onder het genot van de nodige biertjes. Daarbij is het in deze dergelijke setting erg lastig de ene groep blonde meisjes te onderscheiden van de andere, en dit is nou net de gemene deler van al mijn vriendinnen.

Een kwartier, dat toch echt wel voelde als een uur, later zag ik dan toch mijn beste vriendin uit de wc's lopen- **Yes**! Ik kon weer met een gerust hart verder feesten maar ik zal de aankomende tijd tijdens mijn avondjes uit de mogelijkheid van het "waar ben je?"-appje zeker niet meer voor lief nemen.

In een tijd waarin je wordt doodgegooid met het feit dat je schermtijd waarschijnlijk te hoog is, en er steeds meer mensen zijn die zweren bij een **social media detox** wil ik dan ook benadrukken hoe heerlijk het eigenlijk is dat we in principe altijd iedereen kunnen bereiken. Ik weet echt niet hoe mensen vroeger ooit uitgingen, iets afspraken of überhaupt in contact kwamen zonder de hedendaagse gemakken van Whatsapp of andere sociale media.

Dus de volgende keer dat je weer aan moet horen dat telefoons je privacy afnemen, dat onze generatie te veel op sociale media zit en dat niet iedereen altijd hoeft te weten wat je aan het doen bent, onthoud hoe fijn het eigenlijk is dat je de optie hebt om dit wél met mensen te delen. En deel op elk avondje uit met je vrienden waar jij bent.

STORING

DINER IN HET OV, GOED IDEE?

Urenlange telefoongesprekken over hoe het weekend was, Big Macs die naar binnen gewerkt worden en mensen die hard aan het studeren zijn; ik heb het de afgelopen periode allemaal voorbij zien komen in de trein. Dagelijks twee uur per dag in de trein heeft me een hoop irritaties en dilemma's opgeleverd. Want wat kan er nu wel of niet in de trein?

TEKST JULIA VAN ZOEST
BEELD ME'SHELL PROVENCE

Het gezeur begint al bij het zoeken naar een vrije stoel. Het vinden van een plek zonder vreemden naast je is natuurlijk de ideale situatie. Helaas maak je het op deze manier bijna nooit mee. Naast een onbekende gaan zitten is op zo'n moment meestal de beste oplossing. Maar ook dit brengt wat problemen met zich mee. Want ondanks dat het zichtbaar is dat er mensen nog een plekje zoeken, zijn er genoeg mensen die hun tas naast zich laten staan in een volle coupé. Vervolgens krijg jij een geïrriteerde blik terug, wanneer je vraagt of ze alsjeblieft hun tas weg kunnen zetten zodat jij kan zitten.

Eenmaal een plaats gevonden, is het altijd maar hopen dat je een goede plek gekozen hebt. Dit blijkt moeilijker dan het lijkt. Er bestaat namelijk altijd een kans dat je medereiziger ontzettend stinkt en jij je hele treinreis je adem moet inhouden om het nog een beetje draaglijk te houden. Natuurlijk kan je ook een andere plek zoeken, maar dit komt ook zo respectloos over. Het andere moment zit je niet in zweetlucht, maar heeft je buurvrouw in de trein bedacht dat het een goed moment is om een BIFI-worstje te eten, wat misschien nog wel erger is dan zweetlucht. Behalve stank, is ook geluidsoverlast een vaak voorkomend probleem in de trein. Veel mensen denken namelijk dat de hele treincoupé het leuk vindt om te luisteren naar hun favoriete muziek of YouTube video's. Of ze weten niet dat je ook oortjes in je telefoon kan stoppen om zo geen geluid te maken in de trein, dat kan natuurlijk ook. Bovendien wordt de trein regelmatig gezien als ideale plek om telefoongesprekken te voeren. Prima natuurlijk, al is het misschien wel een beetje asociaal om de hele trein een uur te laten luisteren naar jouw telefoongesprek. Toch moet ik eerlijk zeggen dat ik het best vermakelijk vind om te luisteren naar mijn medereiziger die een uur praat over hoe afschuwelijk ze haar nieuwe collega vindt en hoe verschrikkelijk ze er afgelopen nacht aan toe was.

Natuurlijk is er altijd de optie om in de stiltecoupé te zitten. De kans is hier alleen groter dat mensen jou als irriterende factor beschouwen. Een hele treinreis voorzichtig doen om deze geïrriteerde blikken jouw kant op te voorkomen, is ook niet bepaald ontspannen. Daarom is het misschien toch het best om tussen de stinkende, etende en bellende mensen, te zitten waar je zelf degene bent die de geïrriteerde blikken kan geven.

DE LUISTERLIJN

De Luisterlijn krijgt elke dag te maken met mensen die iets kwijt willen en hun hart luchten bij de Luisterlijn. De vrijwilligers van de Luisterlijn horen dan veel privé informatie die niet in verkeerde handen mag vallen. Niet echt een makkelijke taak, zeker als het gaat om heftige informatie. Hoe gaan zij om met deze gevoelige informatie? En hoe privé is zo'n gesprek eigenlijk? Dit zochten wij uit, dus lees snel verder om er precies achter te komen wat er met jouw informatie gebeurt na een gesprek met de Luisterlijn.

TEKST SAMANTHA VAN CADSAND & EVA GERRITSEN
BEELD ANOUK VAN BOKHOVEN

WAT DOET DE LUISTERLIJN EN VOOR WIE?

De Luisterlijn is er voor mensen die in hun eigen omgeving niet met hun verhaal terecht kunnen, willen of durven. Door de bereikbaarheid (24 uur per dag, 365 dagen per jaar) en de geboden anonimiteit, is de Luisterlijn letterlijk bereikbaar voor iedereen die behoefte heeft aan een luisterend oor, een gesprek 'van mens tot mens'. De doelgroep is breed. Of je nou 80 jaar bent of 20, iedere inwoner van Nederland kan bij de Luisterlijn terecht.

Alles wat er zich in een mensenleven kan voordoen komt voorbij, dus de Luisterlijn richt zich niet op een specifiek probleem of gevoel. De meest voorkomende thema's zijn eenzaamheid, geestelijke gezondheid, psychosociale problemen en relatieproblemen. Mensen mogen dan ook vrijwel overal over praten en hoeven zich door de strenge regels wat betreft anonimiteit geen zorgen te maken over hun privacy.

SAMENWERKING MET ANDEREN

Hoe vindt de Luisterlijn de geschikte mensen voor deze taak? De Luisterlijn werkt veel met vrijwilligers. Zij hoeven niet een bepaalde achtergrond te hebben met een bepaald opleidingsniveau of iets dergelijks. Vrijwilligers voeren gesprekken van mens tot mens en zijn geen hulpverleners of deskundigen. Of iemand nu een huisvrouw of advocaat is, iedereen die goed kan luisteren en minimaal één dienst per week kan draaien is welkom. Voordat vrijwilligers aan de slag gaan, krijgen ze eerst een uitgebreide training.

De training bestaat uit een e-learning gedeelte en diverse praktijkbijeenkomsten waarin vooral gesprekken worden geoefend. Belangrijk is om niet dingen voor anderen in te vullen, het gaat erom dat de mensen een luisterend oor hebben om mee te praten, advies geven gebeurt dan ook alleen als de situatie daarvoor vraagt, bijvoorbeeld als iemand elders beter terecht kan. De Luisterlijn bundelt waar mogelijk de krachten met andere organisaties zoals de 'Nationale Coalitie tegen Eenzaamheid' en '113Zelfmoordpreventie".

HET TRAINEN VAN MEDWERKERS

De Luisterlijn zegt altijd: "iemand moet plek hebben in zijn hoofd, hart en agenda". Daarbij zijn ook empathie en leergierigheid belangrijk. Naast de uitgebreide training wordt van iedere vrijwilliger verwacht dat diegene absolute geheimhouding in acht neemt over wat diegene hoort of leest. Bij de start van de samenwerking moet daarom een een **geheimhoudingsverklaring** worden getekend.

Dit betreft ook de identiteit van collega's en interne informatie van én over de organisatie. De telefoongesprekken worden nooit opgenomen.

Anonimiteit is een recht en geen plicht. Deze anonimiteit zorgt ervoor dat moeilijke dingen bespreekbaar worden en het biedt veiligheid voor de gesprekspartner om te uiten wat diegene anders vaak niet durft te vertellen. Daarom is het zo'n belangrijk uitgangspunt van de Luisterlijn.

GEHEIMHOUDING VAN GEGEVENS

Een gesprekspartner hoeft diens naam of andere NAW-gegevens niet aan vrijwilligers te vertellen. Mocht de gesprekspartner wel gegevens over zichzelf of andere herleidbare personen melden, dan mogen deze nooit worden gedeeld. Op de website kan men **anoniem** hun verhaal delen, anders dan het één-op-één gesprek waar de Luisterlijn bekend om staat. Ook hier is *privacy* enorm belangrijk. Er wordt zorgvuldig omgegaan met de persoonsgegevens, daarbij houdt de Luisterlijn zich aan de bestaande wet- en regelgeving op het gebied van *privacy*. De persoonlijke verhalen worden dus alleen met toestemming gedeeld en bevatten **geen** persoonlijke of andere herleidbare gegevens. Voor het terugtrekken van het gedeelde verhaal, het inzien, wijzigen of verwijderen van persoonsgegevens kan een schriftelijk verzoek ingediend worden bij de functionaris gegevensbescherming van de Luisterlijn.

Als vrijwilligers een lastig, naar of moeilijk gesprek hebben gehad en stoom willen afblazen of niet verder kunnen, dan kunnen ze contact opnemen met hun trainer/begeleider of met de vrijwillige achterwacht. Intern worden de verhalen die vrijwilligers horen ook niet gedeeld. Sommige gesprekken worden wel **onherleidbaar** besproken tijdens begeleide intervisie met de trainer en eventueel andere vrijwilligers. Hier gaat het om lastige of moeilijke gesprekken. Deze intervisie is bedoeld om de kwaliteit van gespreksvoering nog beter te maken.

HOE WERKT HET SYSTEEM?

De Luisterlijn heeft wel fysieke locaties, maar het is een landelijke organisatie. Het lokale nummer kan gebeld worden, maar of je iemand uit de regio aan de lijn krijgt, is afhankelijk van of er een vrijwilliger op die locatie beschikbaar is. Zo niet, dan word je automatisch doorverbonden naar een andere locatie, mogelijk uit een andere regio. Ook is er een landelijk telefoonnummer: 088 0767 000. Sowieso ziet de vrijwilliger het nummer van de beller niet. Telefoonnummers komen gecodeerd binnen, dus niemand binnen de organisatie heeft inzage in het nummer waarmee gebeld wordt. Zelfs als iemand met 'nummerweergave aan' belt, wordt het niet gezien. Wel worden de telefoonnummers versleuteld opgeslagen in het systeem. Natuurlijk kan je ook via chat of mail je verhaal doen. Ook dan is het IP-adres en/of e-mailadres niet zichtbaar voor de vrijwilligers of andere medewerkers van de organisatie. Het IP-adres en e-mailadres worden ook versleuteld opgeslagen in het systeem.

Dit is een **extern systeem** bij een externe *provider*. Het systeem is dus niet toegankelijk voor de Luisterlijn-medewerkers. Anonimiteit wordt alleen geschonden als derden in gevaar zijn, dan kan dit bij de politie worden gemeld. Dit is wel erg uitzonderlijk. Het herleiden van versleutelde persoonsgegevens kan alleen aanvangen op basis van een verkregen 'Vordering Identificerende Gegevens' conform **Artikel 126nc Wetboek van Strafvordering** van een Officier van Justitie door de externe *providers*. In andere situaties zal de anonimiteit niet zonder toestemming van de gesprekspartner worden geschonden. De vrijwilliger zal mogelijkheden kunnen bieden voor hulp en deze met de beller bespreken, mocht die een gevaar zijn voor zichzelf. Wel blijft die anoniem als diegene de hulp niet accepteert. Er wordt niet doorverbonden naar hulpdiensten of op een andere manier contact met hen gelegd.

Door dag en nacht een luisterend oor te bieden, stelt de Luisterlijn mensen in staat om zorgen, pijn en verdriet te delen met iemand.
De Luisterlijn is bereikbaar via telefoon (**088 0767 000**), chat en e-mail (**deluisterlijn.nl**).

de luisterlijn
wij geven gehoor
088 0767 000

TRENDS: LEKKAGE

Lekkage: het lekken van data, geheimen, roddels, noem het maar op. Wat is er tegenwoordig eigenlijk allemaal trending op dit gebied? Wij hebben voor jullie de nieuwste 'lekkage trends' op een rijtje gezet.

TEKST JULIA VAN ZOEST & FLEUR PETERS
BEELD ME'SHELL PROVENCE

PODCASTS

1. CYBERHELDEN

Podcasts zijn niet meer weg te denken tegenwoordig! Ook over onderwerpen als cybersecurity en roddels bestaan series en podcasts. Ronald Prins gaat in zijn podcast "Cyberhelden" in gesprek met de grootste *cybersecurity* helden van Nederland! Vanuit zijn werk in de wereld van cyberbeveiliging is hij dagelijks in contact met mensen die er alles aan doen om de data van grote bedrijven en instanties te beschermen. Ben je benieuwd naar hoe dit allemaal werkt? Er staan maar liefst 52 afleveringen met deze helden online! Nieuwsgierig geworden naar deze podcast? Lees dan gauw het interview!

2. DATABAR

Robert van Straalen en Berend Dumas werken allebei als *data scientist* voor *Data Science Lab*. Dit bedrijf zet zich in om data in te zetten als waardevolle kennis. Een tijdje geleden zijn deze twee wetenschappers een podcast gestart: De Databar. Samen met verschillende gasten nemen Robert en Berend je mee in de wereld van *data science*. In hun afleveringen bespreken ze de mogelijkheden en moeilijkheden van de laatste innovaties op het gebied van technologie. Deze podcast brengt je veel nieuwe kennis bij op een redelijk luchtige manier. Een leuk weetje is dat deze podcast daadwerkelijk wordt opgenomen in een eigen bar van *Data Science Lab*. Inmiddels staan er acht afleveringen online en er komt ongeveer iedere maand een nieuwe aflevering bij.

3. STRIKT PRIVÉ

"Privé" staat vooral bekend als een bekend Nederlands roddelblad. Privé is dan ook het meest gelezen roddelblad van Nederland. Wat veel mensen misschien niet weten, is dat het tijdschrift ook een podcast heeft. In deze podcast houden Jordi Versteegden en Evert Santegoeds, beiden entertainment journalist van beroep, je op de hoogte van het laatste entertainmentnieuws. Daarnaast geeft deze podcast je een kijkje achter de schermen bij het weekblad en krijg je bijna dagelijks een update van het laatste nieuws uit showbizzland.

JUICE KANALEN

Wat we niet mogen vergeten is dat er ook de andere kant bestaat van het beschermen van geheime gegevens, namelijk het verspreiden van deze gegevens. Kanalen die roddels verspreiden van BN'ers zijn tegenwoordig niet weg te denken uit onze mediawereld en daarom hebben wij de meest uitgelichte kanalen hieronder genoemd voor jullie.

1. LIFE OF YVONNE

De 38-jarige Yvonne Coldeweijer heeft sinds een aantal jaren haar eigen juicekanaal. Hier deelt ze dagelijks roddels over bekende Nederlandse acteurs, influencers, voetballers, zangers, noem het maar op. Wanneer je twee BN'ers hand en hand over straat ziet lopen en je dit normaal zou vertellen aan je vrienden, kan je dit nu opsturen naar Life of Yvonne en staat het binnen no-time op haar kanaal. Daar waar traditionele media twee keer moeten nadenken voor ze hun vingers branden aan geheimen en juicy details, worden deze zonder pardon door Yvonne op het internet verspreid. Dus of deze roddels altijd waar zijn is aan jou als kijker zelf te bepalen, maar wil je nou altijd op de hoogte zijn van het snelste nieuws? Dan weet je waar je moet kijken.

2. RODDELPRAAT

Ook het duo Dennis Schouten en Jan Roos maken video's waarin ze geruchten en foto's van bekende Nederlanders naar buiten brengen. In een klein kantoortje in Amersfoort neemt het duo iedere woensdag een video op die ze posten op hun YouTube-kanaal waarin ze de laatste roddels vertellen, met naar hun eigen zeggen "een goed gevoel voor humor". Je moet hierbij niet denken aan een "Hilversums goedgekeurd praatje", maar aan een parodie met snoeiharde humor. Dit leidt dan ook af en toe tot een rechtszaak doordat ze door de door hen besproken showbizz zaken voor de rechter worden gesleept, maar dat hoort er aldus Jan Roos "gewoon een beetje bij". Het doel van RoddelPraat is en blijft een kanaal waar je om hoort te lachen, door veelal harde humor waarbij roddels over BN'ers of onzinnige personen iets worden aangedikt.

DAY IN THE LIFE OF...

JASPER MAATMAN

TEKST LOTTE MEEUSE
BEELD ANOUK VAN BOKHOVEN

Waar CW-studenten nog leven van tentamen naar deadline, komt er ooit een tijd dat we onze dromen kunnen najagen. Na de studie Communicatiewetenschap zijn er talloos veel mogelijkheden in waar je terecht kunt komen. In de rubriek 'Day in the life of…' interviewen we iedere editie een CW-alumnus. Deze editie: Jasper Maatman! Van de master Commerciële Communicatiewetenschap naar Vertigo 6. Hoe is dat gegaan?

Loopbaan

In 2014 begon Jaspers studententijd. Aan de Hogeschool Saxion volgde hij Commerciële Economie met binnen de opleiding focus op sport en vrijetijdsbesteding. Daarna begon zijn tijd bij de Radboud Universiteit: in 2019 volgde hij de pre-master Communicatiewetenschap en in 2020 volgde hij de master Commerciële Communicatiewetenschap. "Ik vind het heel interessant hoe je mensen gaat overtuigen van een product, vooral creatieve marketingcampagnes spreken mij aan. Ik wil eerst alle kanalen van online marketing volledig onder de knie krijgen, waar ik over een paar jaar sta, is lastig te zeggen. Vooral tijdens mijn studie heb ik nooit verder gekeken dan één jaar: eerst de punten maar halen en dan zie ik wel weer verder."

Vertigo6

"Via een online marketing *traineeship* ben ik uiteindelijk bij Vertigo 6 terechtgekomen, dat is toen allemaal heel snel gegaan. Drie weken na het eerste gesprek kon ik er al aan de slag. Zij hadden de mogelijkheid om te groeien en eigenlijk klikte het gelijk allemaal goed." Vertigo 6 is een Marketing- & PR- bureau met grote klanten zoals Logitech en EA. Ze werken veel met influencers samen en adverteren via sociale media en Google. Ze organiseren ook wel eens PR-evenementen. Mooie voorbeelden zijn een *pop-up store* op Utrecht Centraal voor de game Saints Row en het NK Muisklikken wat door alle landelijke radiostations is opgepakt. "We zitten zoveel mogelijk op *awareness*. We richten ons op het aanwezig zijn en bekend maken van een merk bij de doelgroep." Als er een nieuw product uitkomt van bijvoorbeeld Logitech, stuurt Vertigo 6 het nieuwe product naar hun contacten die geïnteresseerd zijn in hardware van Logitech. Als zij de producten dan willen reviewen, krijgt het nieuwe product dus ook media-aandacht. Daarnaast zetten ze influencers in om de doelgroep op een juiste manier te bereiken en aan te spreken.

Werkdag

Niets zo divers als de baan van Jasper. Zijn werkdag verschilt per periode, maar hij houdt zich voornamelijk bezig met het adverteren via Google: bijvoorbeeld *search*, *display*, en YouTube. Ook adverteert Jasper op verschillende sociale media, zoals Facebook, Instagram, TikTok en Pinterest.

Over de sfeer op de werkvloer heeft hij ook niets te klagen. "Het bedrijf zelf is super informeel en gezellig. We hebben allerlei uitjes, en iets dat we vaak doen is een FIFA-toernooi. EA is een van onze klanten, hun grootste spel is FIFA, dus dat wordt door ons bijna elke pauze gespeeld."

Tips

Of Jasper de huidige studenten nog iets wil meegeven? "Stage lopen vond ik heel leuk om te doen, omdat je van alles kunt uitproberen. Je komt erachter wat je wilt, maar ook wat je niet wilt. Ga gewoon kijken wat je leuk vindt en of iets je bevalt, zo niet dan streep je dat af en vind je vanzelf iets dat je wel leuk vindt!"

DE GROTE 'HOE VEILIG ZIJN JOUW GEGEVENS?' QUIZ

TEKST EVA GERRITSEN
BEELD ANOUK VAN BOKHOVEN

Heb jij voor elk account een ander wachtwoord en gebruik je twee factor authenticatie? Of zoek je nu snel even op wat dat eigenlijk betekent? Doe de quiz en kom erachter hoe veilig jouw gegevens op het internet zijn.

Hoeveel verschillende wachtwoorden heb jij?
A ik gebruik één wachtwoord of een variatie hiervan voor al mijn accounts (1 punt).
B ik wissel af tussen een paar verschillende wachtwoorden (2 punten).
C ik gebruik voor elk account een ander wachtwoord (3 punten).

(-1 als je een van de volgende gegevens in je wachtwoord hebt staan: geboortedatum, naam huisdier, eigen naam).

Ik gebruik een VPN…
A altijd als ik niet op mijn eigen netwerk zit (3 punten).
B alleen als ik artikelen van de uni nodig heb (2 punten).
C nooit (1 punt).

Ik gebruik twee-factor authenticatie…
A Voor overheidsaccounts (2 punten).
B niet (1 punt).
C Voor al mijn belangrijke accounts (3 punten).

Mijn Instagram account is…
A openbaar (1 punt).
B privé (3 punten).
C openbaar maar met een privéverhaal (2 punten).

Als ik een melding krijg om mijn apparaten te updaten doe ik dit…
A gelijk (3 punten).
B na een aantal keer uitstellen (2 punten).
C alleen als het écht moet (1 punt).

Tel je punten en kom erachter hoe veilig jouw gegevens op het internet zijn!

12 - 15 punten
Jij bent super veilig op het internet! Je bent een expert in het maken van wachtwoorden en weet alle tips en *tricks* als het gaat om twee factor authenticatie en VPN's. Probeer deze kennis eens te delen met je vrienden die hier misschien niet zoveel vanaf weten, zo help je hen ook een stapje verder.

8 - 11 punten
Jij neemt redelijk wat maatregelen om je veilig op het internet te begeven, maar weet ook nog niet alle *hacks* die er zijn. Wie weet staan er in de '*How to*'-rubriek nog tips die jou helpen om nóg veiliger te internetten.

4 - 7 punten
Oei, jij kan nog wel wat meer doen om je online gegevens te beveiligen. Het klinkt misschien ingewikkeld, maar het hoeft echt niet zo moeilijk te zijn als je denkt. Kijk bijvoorbeeld eens bij de tips om veiliger te internetten in de '*How to*'-rubriek.

DATA DON'TS

Privacy is iets wat de meeste mensen heel erg waarderen. Niemand zou het waarschijnlijk prettig vinden als je woonadres overal op het internet zou staan, of dat iedereen zomaar een kijkje kan nemen in je browsegeschiedenis. We zijn dus heel erg gesteld op onze privacy, maar toch doen we dagelijks veel dingen (onbewust) die onze privacy in gevaar kan brengen. Wil jij weten wat dat is? Lees dan vooral verder!

TEKST SAMANTHA VAN CADSAND & EVA SLOT
BEELD FLOOR CROUSEN

1. Cookies accepteren

Cookies zijn databestanden die bijhouden of je apparaat weleens hun website heeft bezocht. Niet-functionele cookies doen echter veel meer en vaak staan deze toe dat de website jouw browsegegevens doorverkoopt aan een derde partij. In het *cookiebeleid* van veel websites staan aanvankelijk vaak die specifieke cookies uit, maar het legitieme belang van derde partijen staat meestal wel aan. Dit is de reden waarom een derde partij data wil kopen, omdat ze zonder cookies natuurlijk geen geld zouden kunnen verdienen. Het is een rechtmatige reden onder de AVG (Algemene Verordening Gegevensbescherming) en een uitzondering wat betreft het geven van toestemming, vandaar dat het automatisch aanstaat. Dit legitieme belang kan meestal toch uitgeschakeld worden, net zoals veel andere niet-functionele en dataverzamelende cookies. De meeste websites bieden deze optie wanneer je de website voor het eerst bezoekt of onderaan de website op het cookiebeleid klikt.

2. Openbare wifi netwerken gebruiken

Openbare wifi is erg makkelijk toegankelijk als het wachtwoord zomaar vrijgegeven wordt. Dit betekent ook dat onze data via dit wifi netwerk makkelijk toegankelijk wordt voor mensen met slechte bedoelingen. Wanneer je bijvoorbeeld Twitter hebt geopend op je telefoon, worden je wachtwoord gegevens en gebruikersnaam doorgezonden. Twitter versleuteld deze data wel, dus mensen kunnen het niet zomaar detecteren, maar niet alle apps versleutelen dit.

3. Social media gebruiken

Google, Facebook, Instagram, Tiktok… We kunnen ons bijna geen leven zonder social media meer voorstellen. Toch zijn deze platforms ook een bedreiging voor je privacy. De bedrijven achter deze platforms maken namelijk volop gebruik van persoonlijke gegevens. Ze bieden hun diensten gratis aan: ze hoeven geen geld van de gebruikers, maar wel informatie. Bijvoorbeeld informatie over jouw woonplaats, sociale omgeving, koopgedrag, inkomen en interesses. Deze informatie verkopen de bedrijven vervolgens door aan adverteerders, zodat zij zorgvuldig samengestelde profielen kunnen gebruiken om gericht te adverteren.

4. Devices gebruiken die 'altijd aan' zijn

Tegenwoordig kan bijna niemand meer zonder devices zoals Alexa, Siri of Google Home. Deze devices staan altijd 'aan', soms zelfs zonder dat we het door hebben, en kunnen makkelijk gehackt worden door een derde partij. Ook kunnen deze apparaten constant meeluisteren met de gesprekken die je voert. Onder deze devices vallen ook diverse camera's. Veel ouders in Amerika hangen een camera in de kamer van hun kind, zodat ze op afstand kunnen checken hoe het met hun baby gaat. Klinkt als een slimme oplossing, alleen zijn deze camera's al meerdere keren gehackt. Dit gaat verder dan alleen begluren, soms konden de hackers zelfs door de camera's dingen fluisteren tegen de baby's.

5. Illegale streamingdiensten gebruiken

Elke keer dat je via illegale linkjes naar je favoriete film of een livestream van een voetbalwedstrijd kijkt, loop je een groot risico. Je loopt namelijk het gevaar om te worden blootgesteld aan gevaarlijke malware, fraude en gegevensdiefstal. Dit risico neemt heel erg toe wanneer je creditcard- of bankgegevens uitwisselt om inhoud te kunnen bekijken op deze illegale sites. Voor je het weet is je bankrekening leeggehaald, dus pas hier goed voor op!

6. Gebruikmaken van AI filters

Op Tiktok is onlangs een filter viral gegaan die je gezicht omtovert tot een Japans manga-figuur. Natuurlijk is Tiktok niet de enige app die dit doet: veel mensen uploaden hun foto's om omgetoverd te worden in een schattig cartoon personage of een held uit je favoriete film. Deze transformatie wordt gedaan door AI (artificial intelligence). Doordat het systeem steeds meer foto's binnen krijgt, wordt AI steeds beter in haar taak. Internetgebruikers die anti-AI zijn waarschuwen ons hiertegen. Wij helpen zo namelijk mee met de ontwikkeling van deze AI, waardoor het steeds beter mensen kan identificeren. Daarnaast vinden veel artiesten en kunstenaars AI een slechte ontwikkeling, aangezien het stukjes van bestaande kunsstijlen samenplakt tot een nieuw kunstwerk. Hierdoor worden kunstenaars dus eigenlijk buitenspel gezet.

7. De incognito modus gebruiken

De incognito modus of private browsing functie kan worden gebruikt als je ergens naar zoekt waarvan je niet wil dat andere gebruikers op dezelfde computer dit weten. Heel eerlijk toegegeven is deze incognito modus op zichzelf niet gevaarlijk voor je privacy. Echter denken veel mensen dat je met de incognito modus anoniem en volledig onherkenbaar bent, maar in de praktijk ben je helemaal niet zo anoniem. Wanneer je deze modus gebruikt, sla je geen zoekgeschiedenis, cookies of wachtwoorden op maar je IP-adres en talloze andere gegevens zijn nog steeds zichtbaar en worden nog steeds het internet opgestuurd. Zo heel erg *incognito* is deze modus dus eigenlijk helemaal niet!

8. Spelletjes spelen op je telefoon

Veel mobiele spelletjes, zoals *Words with Friends* en *Farmville*, volgen en registreren persoonsgegevens zoals de voor- en achternaam, contacten uit je adresboek, IP-adressen en inhoud van chats tussen spelers. Het is onduidelijk of deze data weer gedepersonaliseerd wordt voordat het aan derden wordt doorverkocht.

9. Je wachtwoorden niet wijzigen of hetzelfde wachtwoord gebruiken

Tegenwoordig zijn er zóveel platforms waar je een account voor moet aanmaken, dat het bijna onmogelijk is om voor elk platform een ander wachtwoord te bedenken en onthouden. Toch is het wel heel belangrijk om voor elk platform een ander wachtwoord te gebruiken. Wanneer je namelijk voor elk platform hetzelfde wachtwoord gebruikt, is het voor hackers heel gemakkelijk om zo in één klap meerdere accounts te hacken. Ook is het van belang om je wachtwoord om de paar maanden te wijzigen, zodat je het voor hackers al helemaal lastig maakt om je wachtwoord te ontcijferen.

10. Een kopie van je ID-kaart mailen

Als je net bent aangenomen bij een nieuwe baan is het geen gekke vraag van je baas om een kopie van je ID op de mail te zetten. Toch is het niet heel slim om dit zomaar te doen, aangezien je mail gehackt kan worden en de hackers vervolgens in het bezit zijn van jouw burgerservicenummer, handtekening en andere gegevens. Gelukkig is dit probleem heel simpel op te lossen! De Rijksoverheid heeft namelijk een app (KopielD-app) ontwikkeld waarmee jij heel makkelijk én veilig een kopie van je ID-kaart kan versturen, zonder dat hackers jouw gegevens kunnen gebruiken.

Hopelijk ben je je nu iets meer bewust van de gevolgen van je mediagedrag op het gebied van privacy. Aan hoeveel van deze tien dingen maak jij je wel eens schuldig? Waarschijnlijk aan behoorlijk veel, omdat deze dingen eigenlijk heel normaal zijn geworden in ons dagelijks leven. De volgende keer dat je een pop-up ziet verschijnen over het accepteren van cookies, zal je hier hopelijk extra goed over nadenken, in plaats van ze zomaar te accepteren!

HOW TO...
PROTECT YOUR DATA

Het internet is niet meer weg te denken uit ons leven. Dit betekent ook dat veel van onze data online staan. Het is dan ook belangrijk om deze goed te beveiligen en dat is makkelijker dan het klinkt. Met deze tips hopen we dat jullie straks allemaal veilig op het internet kunnen surfen.

TEKST SAMANTHA VAN CADSAND & EVA GERRITSEN
BEELD FLOOR CROUSEN

TIP 1
Beperk samenwerking mappen, gedeelde albums of gedeelde afspeellijsten

Zo is op Google Docs het beter om specifieke mensen toe te voegen dan een link vrij te stellen voor iedereen, want deze kan makkelijk op het internet terecht komen. *Trolls* vinden het leuk om gezamenlijk afspeellijsten aan te passen en hier liedjes aan toe te voegen, dat maakt de gezamenlijk Spotify playlist voor uitjes een stuk minder gezellig. Spotify biedt geen rapporteer optie voor spam en deze accounts blokkeren helpt meestal maar even, uiteindelijk leidt het zelfs tot nog meer *trolls*. Dan is het wellicht toch beter om deze afspeellijsten privé te maken zodra dit gebeurt.

TIP 2
Gebruik willekeurige Googlewachtwoorden

De meeste mensen gebruiken steeds hetzelfde wachtwoord, met een kleine verandering hier en daar om te voldoen aan de wachtwoordregels van de website waar we een account aanmaken. Erg verstandig is dit niet, omdat dit heel makkelijk is voor anderen om te raden. Een hacker kan nadat hij bij één account het wachtwoord heeft gekraakt, makkelijk in al je andere accounts komen. Gelukkig zijn Google en Google Chrome wachtwoorden (wanneer ze automatisch gegenereerd zijn) geëncodeerd met een geheime sleutel die voor elk apparaat anders is. Zo kan niemand hetzelfde wachtwoord krijgen als die van jou of deze makkelijk kraken met een eigen *software*.

TIP 3
Zet je bluetooth uit als je het niet gebruikt

Veel apparaten die we gebruiken werken tegenwoordig met bluetooth. Vaak heel handig, bijvoorbeeld om een draadloze koptelefoon te gebruiken. Maar als je dit apparaat niet meer gebruikt, zet je je bluetooth dan gelijk weer uit? Het is beter om dit wel te doen, omdat je telefoon anders makkelijk gehackt kan worden. Hackers kunnen met hun eigen bluetooth-apparaat verbinding maken met jouw telefoon en krijgen zo toegang tot alle bestanden die erop staan. Het risico is vooral aanwezig op drukke plekken, want een hacker moet binnen 15 meter van jouw telefoon zijn om verbinding te kunnen maken. Geen zorgen, als je bluetooth apparaat al verbonden is met je telefoon kan er geen ander apparaat verbinding mee maken. Je kunt dus gewoon draadloos naar muziek blijven luisteren.

TIP 4
Gebruik ezelsbruggetjes, maar houdt het random

Wat als je niet een wachtwoord kan genereren, maar er zelf eentje moet bedenken? Natuurlijk kan het wachtwoord dan niet te moeilijk zijn, omdat Google het niet voor je onthoudt. Er zijn veel blogposts en andere websites met aanraders over hoe je een wachtwoord hoort te kiezen. Ze raden ezelsbruggetjes aan, zoals de afkorting van een slogan die jij veel gebruikt. Ze raden aan om hier willekeurige nummers doorheen te plaatsen en het wachtwoord minstens 10 karakters lang te maken, met ook andere tekens erdoorheen. Dit kunnen datums zijn die voor jou iets speciaals betekenen, om het makkelijker te onthouden. Maar veel misdaad programma's hebben laten zien dat datums die iets voor je betekenen makkelijk te raden zijn, dus ook deze kunnen het beste door elkaar gehusseld worden.

TIP 5
Stel een biometrisch wachtwoord in voor het ontgrendelen van belangrijke apps

Een voorbeeld van een biometrisch wachtwoord is de vingerafdruk. Een ander voorbeeld is Apple's Face ID. Deze zijn veel moeilijker te hacken dan een wachtwoord, vandaar dat veel telefoons maar ook bankapps deze gebruiken. Sommigen beweren dat een vingerafdruk veiliger is dan Face ID, omdat gelaatstrekken niet compleet uniek zijn, terwijl vingerafdrukken dit wel zijn. Apple experts beweren echter dat hun Face ID 20 keer veiliger is dan een vingerafdruk. Welke je ook kiest, het zal veiliger zijn dan een wachtwoord. Wel is het vaak dat apps en telefoons die dit toestaan ook een optie geven om de vingerafdruk te vermijden door een wachtwoord in te voeren, in het geval dat de vingerafdruk niet meer werkt. Daarom blijft een sterk wachtwoord belangrijk.

TIP 6
Bescherm je wifi-wachtwoord

Onze routers verwerken veel gevoelige informatie. Met de Twitter-app open worden continu de gebruikersnaam en het wachtwoord uitgezonden. Twitter versleutelt deze, maar het is niet te verwachten dat elke app dat doet. Met een wachtwoord dat vrijgegeven wordt (denk aan restaurants) liggen zo privégegevens, wachtwoorden en financiële gegevens voor hackers voor het oprapen. Daarom is het slim om niet in de collegezaal te shoppen, maar thuis. Dit wachtwoord kan beter beschermd worden. Verander daarom het wachtwoord niet naar een persoonlijke (en voorspelbare), zoals de naam van een hond, maar houdt het willekeurig. Het is beter om bij elke bezoeker het wifi-wachtwoord zelf in te voeren dan het sturen van een QR-code, want deze kan namelijk onderschept worden of op het internet terecht komen.

TIP 7
Apps regelmatig updaten en ongebruikte apps verwijderen

Apps willen continu geüpdatet worden voor de minste redenen, maar soms is dit ook echt nodig. Zo was in 2014 Angry Birds gehackt door niemand minder dan de Amerikaanse inlichtingendienst NSA. Deze kwetsbaarheden werden snel met een update opgelapt. Zelfs de overheid is uit op onze data, via de meest onconventionele wegen. Apps die niet gebruikt worden, kunnen onbewust wel data verzamelen. Beter verwijderen dan maar!

TIP 8
Een VPN gebruiken

Hiermee moeten we wel opletten. De meeste VPN's die gratis zijn, kunnen makkelijk geëxploiteerd worden door hackers. Sommigen verzamelen ook zelf data om deze vervolgens door te verkopen. Het beste is om een geverifieerde en betaalde VPN te gebruiken of eentje uit een land met strenge privacyregels die het verzamelen van data zonder toestemming niet toestaan.

Hoeveel van deze tips volg jij nu al op? Hopelijk hebben we je nog iets nieuws kunnen leren en kan je voortaan met een veilig gevoel internetten.

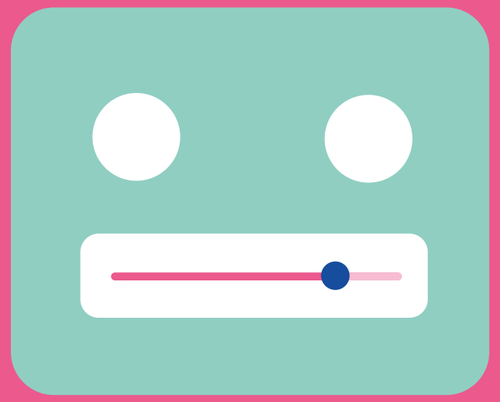
WHAT DO THE SOCIALS SAY?

In deze versie van 'What Do The Socials Say' stelden we jullie weer een aantal vragen via ons Instagram account (@freemcw). Accepteren jullie altijd maar die cookies? En hoe zorg je voor je online veiligheid? Lees snel verder om hierachter te komen en misschien wel je eigen antwoord terug te lezen. Wil je de volgende keer ook met jouw antwoorden in de Freem? Vergeet dan niet om ons Instagram account te volgen!

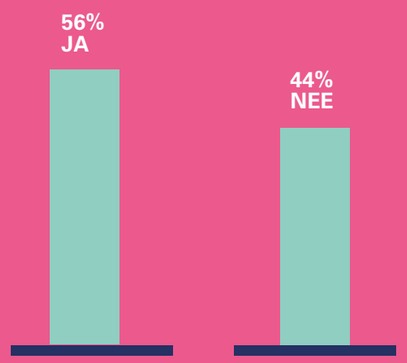
TEKST FLOOR CROUSEN **BEELD** LIEKE SPEE

VRAAG 1: HOE GOED KAN JIJ EEN GEHEIM BEWAREN?

Kan jij heel goed een geheim bewaren? Of ben jij een echte roddeltante, die alles meteen door verteld? Myceliumleden denken in ieder geval dat zij het wel goed kunnen.



VRAAG 2: ACCEPTEER JIJ ALTIJD DE COOKIES?

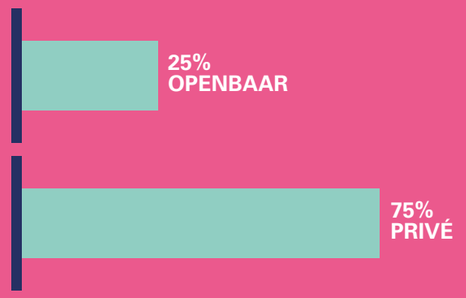


Ook een kleine meerderheid bij onze myceliumleden drukt het liefst meteen op die accepteer knop. Alles weigeren is toch ook veel te veel moeite?! Toch zouden wij als Communicatiestudentjes beter moeten weten.

VRAAG 3: WAT VIND JIJ VAN RODDELKANALEN? EN HEB JE EEN FAVORIET?

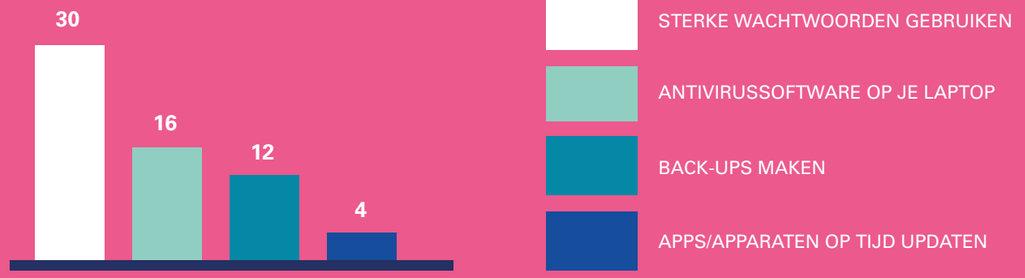
Love it or hate it: roddelkanalen. Ook onder Myceliumleden ontstaan er gemixte reacties. Aan de ene kant heel irritant en storend, maar aan de andere kant toch stiekem wel vermakelijk?

VRAAG 4: WAT VOOR INSTAGRAM ACCOUNT HEB JIJ?



Vindt je het vervelend als iedereen een kijkje kan nemen op je Instagram account? Of vindt je dat juist wel leuk? Bij onze vereniging zijn mensen niet zo'n open boek en zetten ze hun account liever op privé.

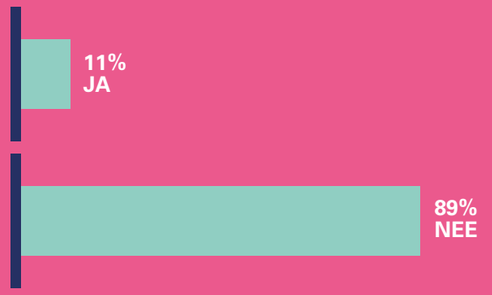
VRAAG 5: HOE ZORG JIJ VOOR ONLINE VEILIGHEID?



Niet alleen je fysieke, maar ook je online veiligheid is tegenwoordig steeds belangrijker. Gelukkig zijn er genoeg dingen die je kan ondernemen die je daarbij helpen. Zo kom je met een sterk wachtwoord al een heel eind!

VRAAG 6: BEN JE WEL EENS SLACHTOFFER GEWEEST VAN EEN SCAM?

Het kan iedereen zomaar overkomen: je wordt opgelicht. De website of dat mailtje zag er wel betrouwbaar uit. Dankzij het internet gebeurd het steeds meer en gemakkelijker. Gelukkig valt het onder alle Myceliumleden nog mee!



OLC UPDATE

TRISTAN BRAAKMAN

ZA-ZIE KUIPERS

EMMY KOK

MIEKE BERENDE

YOUP JANSEN VAN DER SLIGTE

JULIA VERMEER

HILDE VAN SCHIJNDEL

TEKST HILDE VAN SCHIJNDEL
BEELD ME'SHELL PROVENCE

Met de start van de laatste periode is het weer tijd voor een OLC-update. Hoe is het de afgelopen weken gegaan, de cursusevaluaties zijn bekeken en misschien zijn we wel opzoek naar jou!

Het OLC heeft de afgelopen maanden veel gepleit voor extra werkplekken tijdens de tentamenperiodes. Dit zal worden geregeld voor de laatste tentamenperiode en hier is het OLC erg blij mee. Voor onze volgende vergadering zijn wij benieuwd waarvoor studenten we of niet naar de campus komen. Specifiek over wat er in het onderwijs moet veranderen om te zorgen dat jullie als studenten blijven komen.

Heb je hier ideeën over, dan kun je ons bereiken via onze Instagram (@OLC_CW) of stuur ons een mailtje naar olc.cw@student.ru.nl.

Aangezien de laatste periode weer is aangebroken, wordt het voor ons ook tijd om weer op zoek te gaan naar onze vervangers. Wil jij je inzetten voor het verbeteren van onze opleiding en heb je ideeën hoe we dit met en voor studenten kunnen doen? Dan zijn wij op zoek naar jou! Wil je meer informatie, kijk dan op onze Instagram of spreek een van ons aan in de wandelgangen. Verdere informatie over de aanmelding volgt snel! Heb je vragen, opmerkingen of verbeterpunten voor de opleidingscommissie? Stuur ons vooral een mailtje, appje of een berichtje via onze Instagram pagina!

IN·DEI·NOMINE·FELICITER

NAWOORD

TEKST Greet van Horen
BEELD Julie van Kerkhoff

Ik denk dat iedereen wel bekend is met het gevoel dat je mogelijk gehackt bent wanneer je telefoon gaat trippen, je Instagram ineens veel meer mensen volgt dan jij hebt aangeklikt en als je op Facebook ineens niet meer in kan loggen. Of van die advertenties op Instagram waar de daadwerkelijke artikelen niks lijken op de foto van de advertenties. Ik wel in ieder geval!

Alles van ons leven staat in deze tijd op onze telefoon op of onze laptop. Van wachtwoorden en privé gesprekken tot persoonlijke informatie. Deze informatie staat nooit helemaal veilig om onze apparaten, wat angstaanjagend is. Dat gevoel van controleverlies is iets wat heel erg eng is. De hedendaagse wereld bestaat en werkt op sociale media, wij als Communicatiewetenschappers weten dat als geen ander. Soms vind ik sociale media ook maar een eng geheel. Je weet niet meer wat wel of niet echt is. Is er wel of geen fotoshop gebruikt? Hebben mensen het echt wel zo naar hun zin als dat het lijkt op hun sociale media? Dit zijn vragen die ik vaak stel als ik op sociale media zit. Stiekem liegen zij de mensen om zich heen en, nog erger, zichzelf voor met zich anders voor doen op sociale media dan ze zijn. Daarbij is er natuurlijk de verstrengde AVG wet waardoor heel veel dingen ook niet zomaar meer gepost mogen worden. Ik kom daar zelf veel mee in aanmerking als secretaris. Soms hebben niet-leden tijdens borrels de neiging om op foto's te gaan staan, die ik daardoor niet kan posten op onze website. Dit zijn allemaal lastige regels, maar wel nodig! Zonder de AVG, de twee-stap verificaties, de wachtwoord eisen etc. zouden onze gegevens niet zo beschermt zijn. Dit klinkt nu allemaal heel zwaar en negatief. Gelukkig heeft sociale media ook een prachtige functie van mensen samenbrengen en het makkelijk maken om te communiceren met de mensen die je lief hebt. Dus ondanks dat het zijn 'donkere' kanten heeft, is het bij basis nog altijd een mooi initiatief.

Growing a better world together

Rabobank