Midden West-Vlaamse Hobby
COMPUTER CLUB ROESELARE

Ons Kompjoeterblad

Jaargang 33 - Nummer 5 - november / december 2018

Nieuwtjes

Midden West-Vlaamse Hobby
Computer Club Roeselare
Skaldenstraat 27
8800 Roeselare

info@hccr.be
http://www.hccr.be

Met steun van ROESELARE IS 'R VOOR JOU

VRIJE TIJDSPAS

Midden West-Vlaamse Hobby
COMPUTER CLUB ROESELARE

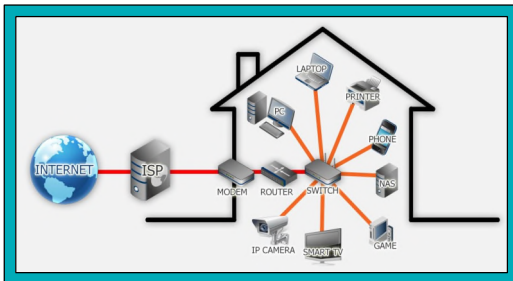
☸ HCCR NIEUWS

* Onze kalender voor - 2018 / 19

3 november 2018
Lightroom

17 november 2018
The hackers are ready, are you !?

1 december 2018
Maak zelf een app voor de smartphone



15 december 2018
Thuisnetwerk, opzetten en configureren

5 januari 2019	
2 februari 2019	Born in the Cloud Thomas Houtekier
2 maart 2019	Photoshop deel 1 door Lisa
6 april 2019	Internet, opfris cursus door Lenny??
4 mei 2019	?? *+ Algemene Vergadering*

19 januari 2019	Synology als Netwerkschijf door Claude *+ Nieuwjaars receptie*
16 februari 2019	Arduino door Peter
16 maart 2019	Photoshop deel 2 door Lisa
20 april 2019	??
18 mei 2019	**Clubuitstap !!** Noteer deze datum nu reeds met stip in je agenda.

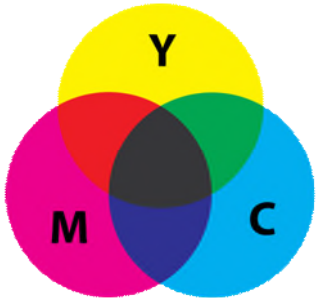
❁ NIEUWTJES

* Trucs om goedkope printerinkt te weren

Printerinkt is peperduur, zeker de officiële fabrieksinkt. Wat voor trucs gebruiken de printerfabrikanten om toch hun dure inkt te verkopen. Hier lees je het!

- ***Tot 75% goedkoper!***

De huismerkinkt van de beste winkels met printerinkt is veel goedkoper dan de originele inkt. Maar de printerfabrikanten doen er alles aan om hun originele inkt te verkopen. Al is deze veel duurder. De besparing op goedkope huismerkinkt ten opzichte van de fabriekinkt is bij laserprinters 50% en bij inktjet printers zelfs 75%. Op de inkt prijs kunnen de printer-fabrikanten het dus nooit winnen. Ze gebruiken andere trucs.



Hier zeven bekende trucs van printerfabrikanten op een rijtje gezet. Plus (*indien van toepassing*) de op-lossing om de trucs te omzeilen.

- ***1. De waarschuwing***

De printerfabrikant waarschuwt in de handleiding en eventueel op het display van de printer zelf dat de namaak cartridges de printer kunnen beschadigen. Onzin, en gewoon negeren.

- ***2. Vervallen garantie***

Hetzelfde geldt voor de garantie die verlopen zou zijn als je "illegale" printerinkt gebruikt. Het hier duidelijk, de fabrikant moet een deugdelijk product leveren en je hoeft je hier dus niets van aan te trekken.

- ***3. Chip op de inktcartridge***

Fabrikanten gebruiken een chip op hun inktcartridges die vooral bedoeld is om te controleren of er wel een fabriekscartridge wordt gebruikt. Als er een nieuw soort cartridge uitkomt moeten de fabrikanten van deze goedkope printerinkt eerst deze chip namaken voor ze cartridges uit kunnen brengen. Hier zal je op moeten wachten.

- ***4. Software-update printer***

De printerfabrikant past de software van de printer aan waardoor je nieuw gekochte printer de goedkope cartridge niet accepteert (*en een oude versie van dezelfde printer wel*). Ook hier valt weinig aan te doen. Je zal moeten wachten tot de aanbieder van goedkope inkt zijn cartridges aan de nieuwe software heeft aangepast. Een operatie die wel een paar maanden kan duren.

- ***5. Houdbaarheidsdatum printerinkt***

Printerinkt heeft een houdbaarheids datum, maar deze datum kan je best wel negeren. Helaas zijn er printers die inkt met een verlopen houdbaarheidsdatum niet accepteren. Hier is niets aan te doen.
Gelukkig gebruiken sommige fabrikanten op hun recente printers deze onzinnige beveiliging niet meer.

- ***6. Cartridge protection***

Fabrikanten zijn heel bezorgt dat kwaadwilligen de printerinkt uit je printer stelen en deze in hun eigen printer gebruiken. Daarom plaatsen ze een beveiliging op de cartridge die er voor zorgt dat hij eenmaal gebruikt in een printer niet meer in een andere printer gebruikt kan worden. Of zouden ze soms bang zijn dat de cartridge wordt hergebruikt? Gelukkig kun je cartridge protection op de printer uitschakelen.

- ***7. Controlelampje***

Anderen gebruiken weer een andere truc op hun printers, in de vorm van een lampje dat alleen gaat branden als de cartridge met printerinkt juist is aangebracht. Bij kloon cartridges gaat dit lampje echter nooit branden, waardoor dit rommel lijkt die nooit goed zit. Maar dat is onterecht, negeer dat niet brandende lampje gerust.

Kijk bij de printerinkt voor de beste en goedkoopste winkels met printerinkt. Daar zie je hoeveel je wel kunt besparen door goedkope huismerkinkt in je printer te gebruiken in plaats van de dure fabrieksinkt.

Bron: fantv.nl

☸ NIEUWTJES

* Een onbeveiligd gastnetwerk voor bezoekers, een goed idee?

Het maakt niet uit of je een hotel, een bistro of een lokaal café uitbaat, consumenten verwachten nu tegenwoordig internettoegang. Het aanbieden van gratis een wifi-verbinding biedt uw zakelijke bezoekers en klanten voordelen, maar een onbeveiligd gastnetwerk opent de deur voor bijkomende problemen en risico's.

Consumenten maken steeds meer en meer gebruik van het internet gedurende hun dagelijkse activiteiten. Bedrijven en organisaties moeten zich daaraan aanpassen en een bijkomende dienstverlening, gratis wifi-toegang, aanbieden. Het is wat klanten willen en het biedt bedrijven tegelijkertijd de mogelijkheid om met klanten te communiceren, het stelt hen in staat om contactgegevens te verzamelen voor toekomstige marketingstrategieën en de organisaties verkrijgen waardevolle klantinzichten. Toch moeten bedrijven goed nadenken over de mogelijke gevaren voor hun organisatie.

- ***Risico's van onbeveiligde netwerken***

Door klanten en gasten toegang te geven tot het internet zonder bijkomende veiligheidsmaatregelen, loopt een bedrijf aanzienlijke risico's. Als die risico's niet worden beperkt, kan het aanbieden van de service gevaarlijk zijn voor een organisatie.

Mogelijk heeft een organisatie een beleid ingevoerd dat betrekking heeft op het toegestaan internet-gebruik door werknemers en zijn die medewerkers zich ook bewust van de beveiligingen of beperkingen die van toepassing zijn op het netwerk.

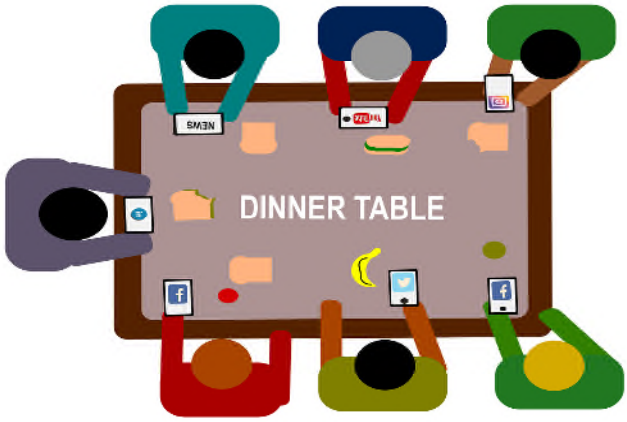
Consumenten, klanten en bezoekers hebben mogelijk een andere opvatting over de beschikbare inhoud en het toegelaten internetgebruik op het wifi-netwerk.

Klanten en bezoekers kunnen bij een gebrek aan controle en genomen veiligheidsmaatregelen profiteren van het wifi-netwerk om toegang te krijgen tot ongepast materiaal zoals pornografie en moreel of ethisch twijfelachtige activiteiten. Daarnaast kunnen ze per ongeluk of, in sommige gevallen, opzettelijk malware of ransomware installeren op het netwerk.
Het gebruik van een beveiligd gastnetwerk kan deze problemen voorkomen.

- ***Bescherm uw klant en uzelf***

Met een beveiligd wifi-netwerk beschermt een organisatie niet alleen de klanten, maar ook zichzelf. Door zakelijke bezoekers en consumenten een beveiligd netwerk aan te bieden, zijn zij ook beschermd tegen 'man-in-the-middle'-aanvallen. Bij die aanvallen onderschept een hacker op een onbeveiligd netwerk het dataverkeer tussen twee of meerdere computers en kan gevoelige data worden gestolen.

Om het hackers moeilijker te maken, is het een goed idee om het draadloze wifi-netwerk te versleutelen en op die manier gegevens en data te encrypteren. Je kan daarvoor gebruikmaken van WPA2-codering om de gegevens en data van bezoekers op het netwerk te encrypteren. Hackers kunnen met de nodige tijd en tools de codering kraken, maar hebben daarvoor wel de toegangscode van het wifi-netwerk nodig.



- ***Netwerk segmentatie***

Als een organisatie een deel van het bedrijfsnetwerk openstelt voor klanten, dan is de beveiliging daarvan geen bijzaak maar een noodzaak. Een bedrijf kan ook best wel gebruikmaken van twee verschillende netwerken, ééntje voor het personeel en ééntje voor bezoekers.

Een scheiding van het beveiligde gastnetwerk en het interne bedrijfsnetwerk bedoeld voor werknemers, is belangrijk om te voorkomen dat onbevoegden toegang krijgen tot mogelijk gevoelige bedrijfsdata. Uitsluitend op het interne bedrijfsnetwerk is het mogelijk en om vertrouwelijke bestanden te raadplegen.

Bedrijven maken daarom gebruik van netwerk segmentatie, een techniek die het mogelijk maakt om een netwerk te splitsen in meerdere subnetwerken en

☸ NIEUWTJES

die subnetwerken of netwerk-segmenten zijn volledig van elkaar gescheiden.

Het is dan ook verstandig om het beveiligde gastnetwerk en het interne netwerk toe te kennen aan een apart netwerksegment. Op die manier kan een bezoeker die beschikt over de inloggegevens geen toegang krijgen tot het interne netwerk voor de werknemers. Cybercriminelen die toegang hebben tot het gast-netwerk, kunnen door de scheiding van data op het netwerk nog steeds niet aan de gevoelige data op het interne bedrijfs-netwerk.

- ***Inhoudfilters***

Een beveiligd wifi-netwerk is een netwerk met opgelegde beperkingen voor de bezoekers die internettoegang verwachten van de organisatie. Het is verstandig om de toegang tot inhoud voor volwassenen te blokkeren. Op die manier word en pornografische content, goksites en andere moreel of ethisch twijfelachtige inhoud geblokkeerd op het netwerk en beschermt een organisatie of bedrijf zichzelf en de bezoekers tegen onbedoelde downloads en malware.

Verder is het altijd een goed idee om de software, firmware en firewall up to date te houden. Op die manier kunnen indringers geen gebruikmaken van bekende kwetsbaarheden in de systemen en is een organisatie beschermd tegen mogelijke kwaadwillige buitenstaanders.

Bron: smartbiz.be

* Facebook datalek trof 50 miljoen accounts

Socialmediaplatform Facebook heeft tot nu toe al een hobbelig jaar gehad en daar werd een nieuwe (en gigantische) hobbel aan toegevoegd. De website werd namelijk getroffen door de zwaarste hackeraanval in zijn geschiedenis, waardoor de hackers in kwestie toegang kregen tot gebruikersdata van bijna 50 miljoen accounts.

Intussen zijn er enkele weken voorbijgegaan en heeft Facebook nog niet kunnen bepalen wat de oorsprong was van de aanval en, of er specifieke accounts uitgekozen werden. Voorlopig lijkt het erop dat het een "algemene" aanval was gezien het enorme aantal getroffen accounts.
Wat volgde na de bekendmaking van dit gebeuren was, in de eerste plaats, algemene paniek en chaos bij Facebook gebruikers die vreesden dat hun gegevens in de verkeerde handen waren gevallen én een daling van 2,6% bij de aandelen van Facebook.

Deze aanval in combinatie met het bekende schandaal van Cambridge Analytica zorgt ervoor dat er wederom een vraag ontstaat naar de veiligheids- en privacy-maatregels voor sociale media. Het antwoord op deze vraag blijft echter nog steeds onbekend.

- ***Het datalek in kwestie***

De geslaagde hackpoging heeft dus voor redelijk wat ophef gezorgd. Maar wat hebben de hackers (*of heeft de hacker*) nu precies gedaan?
Wel, op 16 september zagen werknemers van Facebook dat er een opmerkelijke stijging was bij de "view as" functie waarmee je kan bekijken wat andere gebruikers kunnen zien wanneer zij jouw profiel bezoeken. Nu zat er een bug in deze functie waardoor gebruikers de foute digitale code kregen. Door deze code kon de persoon die "view as" aan het gebruiken was, berichten plaatsen en browsen door andermans account. De hacker zou hierdoor ook toegang hebben gekregen tot sites en apps van derden waaraan een Facebook-account was verbonden.

- ***De reactie van Facebook***

Facebook heeft na de aanval de digitale sleutels van de getroffen accounts gereset en als voorzorgsmaatregel "view as" tijdelijk uitgeschakeld. Door de grote hoeveelheid onrust bij gebruikers ontstond er ook een grote stroom aan berichten en artikels van nieuwswebsites over het voorval. Deze werden soms echter geblokkeerd omdat de systemen van het platform deze grote hoeveelheid gelijkaardige inhoud beschouwden als spam. Intussen is dat probleem ook opgelost en heeft Facebook zich hiervoor verontschuldigd.

Tot slot heeft Facebook naast de klachten en boze berichten ook enkele rechtszaken cadeau gekregen door de hackaanval. De concrete gevolgen hiervan zijn nog niet duidelijk, maar rooskleurig is de toekomst van het sociale mediaplatform in elk geval niet.

Bron: techpulse.be/

☸ NIEUWTJES

* Hoe kwetsbaar zijn we in de cloud? - Enkele misvattingen over cloud security

Elke dag hoor je nieuws over een nieuwe hacks, datalekken en over persoonlijke informatie die wordt gestolen. Allemaal dankzij moderne technologie. Want de rush om die nieuwste technologieën te gebruiken brengt – naast de voordelen – ook vele gevaren mee. Zeker in de cloud. Want die is niet zo veilig als we allemaal denken.

De voordelen van digitale transformatie zijn duidelijk; organisaties zijn nu in staat sneller te innoveren, sneller apps en diensten te lanceren tegen een fractie van de kosten. Daarbij maken ze allemaal gebruik van de cloud. Focus ligt op functionaliteit van de aangeboden diensten: het moet snel gaan, het moet er mooi uitzien en goed werken. Er is minder aandacht voor de veiligheidsaspecten van de tool.

Voor de ontwikkelaars is security eigenlijk een blok aan het been. Alles moet in realtime, en een app mag geen onderbreking of vertraging door security-protocols ondervinden. Echte updates zijn niet meer nodig: developers lanceren gewoon een nieuwe versie van de app met één druk op de knop. En dat geeft frictie met de mensen van security die, terecht, verwachten dat het protocol wordt gevolgd.

- ***Is de cloud-omgeving altijd veilig?***

Cloud providers hebben ons, klanten ervan overtuigd dat de cloud veilig is. Maar klopt dat wel?
Nee, een cloudomgeving wordt continu aangevallen. We zien ook steeds meer geavanceerdere en geautomatiseerde aanvallen, én nieuwe aanvallen met als doel toegang tot de data krijgen, of computerkracht 'stelen' voor bitcoin mining (*waarbij de hackers de processorkracht bewust kunstmatig laag houden zodat het gebruik niet zichtbaar is*).

We deden een test waarbij we cloud services gebruikten en nagingen of de gebruikte settings voldoende waren. We hebben hiervoor een server in de cloudomgeving van een provider opgezet en deze aan het internet gekoppeld. Om nog beter te kunnen analyseren hebben we er nog een HoneyPot voor geplaatst. Na 15 minuten waren al 149 aanvallen gedetecteerd. Na een week telden we bijna 4 miljoen pogingen!

- ***Gedeelde verantwoordelijk-heid***

Heel veel bedrijven hebben zo'n overeenkomst met cloud providers waarin staat dat hun datacenters zeer veilig zijn. Maar die cloud providers zijn niet voor alles verantwoordelijk. Cloud providers zijn verantwoordelijk voor de veiligheid ***van*** de cloud. De klant is verantwoordelijk voor de veiligheid ***in*** de cloud: hij moet ervoor zorgen dat zijn data beveiligd zijn en moet ervoor zorgen dat zijn apps veilig zijn. Het gaat dus om een shared responsibility model. Een verantwoordelijkheid die, zeker met het oog op de GDPR-regelgeving, zeer belangrijk is.

- ***Je bedrijf weg!***

Vele nieuwe business zitten volledig in de cloud. Denk maar aan Uber, Netflix of andere business zoals reisplatformen die in een virtuele omgeving draaien. Je ziet nieuwe autonome aanvalsvectoren opduiken die zich een toegang tot de admin willen verschaffen. Want eenmaal ze die in handen hebben, kunnen ze het bedrijf eigenlijk overnemen. Stel dat als zaakvoerder je eigen wachtwoord weg is en/of je credentials zijn gestolen, heb je dan wel nog een bedrijf? Zo is er nog niet over nagedacht, maar het is een reëel gevaar.

- ***Vier basisprincipes***

Om dit allemaal te voorkomen geven we je nog tot slot vier basisprincipes mee die je in acht moet houden om de cloud effectief te beveiligen.

Vertrouw op een uitgebreide, gelaagde beveiliging die zowel de bekende als de onbekende malware (*en zero-day attacks*) kan detecteren.

Het moet alles heel eenvoudig te implementeren en te bedienen zijn. Niet alleen door security-specialisten maar ook door DevOps of deskmedewerkers. Dat kan door implementaties met één klik en door een doorgedreven automatisering van de tools.

Dynamische security saanpak: de cloud heeft een dynamisch karakter, dus moet de context informatie over de infrastructuur, gebruikers, bedreigingen, gedeeld en geanalyseerd worden zodat men snel en automatisch wordt gewaarschuwd en de policy kan aanpassen aan eventuele wijzigingen in de cloud-omgeving.

Steeds meer bedrijven werken in een hybride omgeving. Bestaande vaste netwerken gecombineerd met meer dan één public cloud provider gaan de architectuur van morgen vormen. Het is dan absoluut noodzakelijk om het overzicht te bewaren. Zorg dus dat je "in the driver seat" zit. Werk daarom met een gecentraliseerd management om te controleren waar alle data en netwerken zich in de cloud bevinden. Werk met logboeken, rapportages en threat intelligence vanuit één enkele beheersconsole.

Bron: smartbiz.be

❁ NIEUWTJES

* Apple Watch Series 4

De Apple Watch Series 4 heeft een groter scherm en een slanker design dan zijn voorgangers. Dit slimme horloge is uitgerust met valdetectie en een ECG-functie. Helaas komt deze functie (nog?) niet naar onze streken. Wat is er nog meer nieuw?

Let op!
Om gebruik te kunnen maken van de Apple Watch Series 4, heb je een iPhone 5s (of nieuwer model) met iOS12 nodig.

De belangrijkste vernieuwing van de Apple Watch series 4 zit aan de buitenkant. Het grotere scherm toont appjes, icoontjes en grafiekjes net wat beter dan de Apple Watch series 3. Het bedienen met je vingers gaat ook lekkerder. De valdetectie is indrukwekkend en is een mooi voorbeeld van hoe de Apple Watch zich steeds meer ontwikkelt tot medisch hulpje.

- ***Nieuw design***

Als je de Apple Watch series 4 naast zijn voorganger legt dan zie je duidelijke verschillen. De horlogekast is kleiner en dunner en het scherm is groter (*30% volgens Apple*). Een klein formaat horloge was 38 mm en is nu 40 mm. De grote is 44 mm en dat was voorheen 42mm.
Het 44 mm horloge voelt ongeveer even zwaar om je pols aan als de series 3 (*de 42 mm variant*), maar ziet er iets slanker uit.

Veel verschil met de vorige versie is er niet, maar het grotere scherm is net wat lekkerder te bedienen. De icoontjes van de apps zijn iets minder priegelig. Daarbij heeft Apple nieuwe horlogeschermen geïntroduceerd waar je meer informatie tegelijk op kunt tonen.

(*) - Hiken of hiking is genieten van een lange wandeling die meestal plaatsvindt in de natuur.

- ***Valdetectie***

De Apple Watch series 4 heeft een vernieuwde gyroscoop en versnellingsmeter. Die stellen het horloge in staat om bewegingen nog nauwkeuriger te registreren. Een concrete toepassing hiervoor is valdetectie. De Apple Watch is in staat om een harde val te herkennen. Zodra het horloge een val met bepaalde impact registreert krijg je een waarschuwing. Die kun je negeren als er niets aan de hand is. Bij nood kun je er 112 mee bellen. Als er binnen een minuut geen actie volgt dan belt de Apple Watch automatisch de hulpdiensten en verstuurt een bericht met locatie.

- ***Hartslag***

De Apple Watch heeft een hartslagmeter om je gezondheid in de gaten te houden. Net als bij vorige modellen meet het horloge continu je hartslag. Dat geeft een goed beeld van je conditie en gezondheid. Nieuw is dat je met het kroontje aan de zijkant een hartritme en ECG-meting kunt doen. Door de Digital Crown 30 seconden aan te raken, krijg je informatie over je hartritme. Je ziet of je hart in een normaal patroon klopt of dat er tekenen zijn van een aan-doening. Alle analyses staan in de Gezondheid-app.
Deze data kun je als pdf met je artsen delen.

De ECG-meting is helaas nog niet beschikbaar. Later dit jaar wordt de app waarmee je dit doet uitgebracht in de Verenigde Staten. Het is niet bekend of en wanneer gebruikers in Europa de dienst kunnen gebruiken.
(ECG = elektrocardiogram)

- ***Sporten***

Met de ingebouwde hartslagmeter en GPS kun je met de Apple Watch een rondje hardlopen of fietsen bijhouden. In het nieuwe besturingssysteem WatchOS5 zitten nieuwe functies voor sporters. De Apple Watch meet nu ook yoga en hiking *(*)*.
Een handige toevoeging is dat het horloge automatisch activiteiten herkent. Zodra je gaat hardlopen, herkent de Apple Watch deze activiteit en stelt hij voor die te meten. Zo hou je alle bewegingen goed bij.

- ***Prijs en verkrijgbaarheid***

De Apple Watch series 4 is er in 2 formaten: 42mm en 44mm (*prijs: €429 en €459).* Er zijn 3 verschillende kleuren: zilver, goud en spacegrijs. De Apple Watch Series 3 is nu verkrijgbaar vanaf €299. Op de site van Apple is de Apple Watch series 1 niet meer te bestellen, maar op internet kom je hem tegen voor €280 (*De Apple Watch 2 is niet meer te koop*).

Bron: Consumentenbond.nl
https://www.apple.com/benl/watch/

☸ NIEUWTJES

* … een en ander

- ***Computer woordenlijst***

Applet, URL, ADSL, .jpg, account … ??!?
Maak je gebruik van een computer dan kan je deze typische termen niet ontlopen.
Voor de ervaren computergebruiker klare taal, maar voor velen onbegrijpelijk.
HCCR probeert u dmv een verklarende woordenlijst wegwijs te maken in de virtuele wereld van het World Wide Web en de computer.

Deze lijst, opgemaakt door onze redactie is er gekomen op vraag van onze leden en kan (*voorlopig*) enkel via onderstaande verkorte url worden bekeken.
https://tinyurl.com/y8krnlbd

- ***Nieuw in iOS 12***

Met de nieuwe iOS 12-app Opdrachten kun je takenreeksen opstellen die je iPhone in het vervolg dan automatisch uitvoert. Zeg bijvoorbeeld, 'Ik ga naar huis', en de iPhone berekent hoelang dat duurt en stuurt je partner ook meteen een berichtje waarin staat hoe laat je thuis bent. De Opdrachten-app staat niet automatisch op je iPhone nadat je iOS 12 geïnstalleerd hebt: je moet de app zelf nog downloaden in de App Store.
Het is eigenlijk een update van de door Apple overgenomen app Workflow.

- ***Luchtige weetjes over allerlei dingen op het internet***

Hier enkele internet feitjes die op het moment dat u dit leest waarschijnlijk al lang weer achterhaald zijn. Heeft u nut werkelijk wat aan al deze informatie gehad?
Zeker: dit benadrukt maar weer hoe belangrijk internet voor een bedrijf (*vereniging*) is. Niet alleen een website is onmisbaar, maar ook social-media is een ontzettend belangrijke factor voor u, uw bedrijf of vereniging.
Met 88 miljard zoekopdrachten per maand is het ook belangrijk dat u website een goede ranking binnen Google heeft.

1. Het internet is in 1969 geboren.
2. Internet is bedacht door het Amerikaanse Ministerie van Defensie.
3. Google verwerkt 88 miljard zoekopdrachten per maand.
4. Yahoo verwerkt 9,4 miljard zoekopdrachten per maand.
5. Elke dag worden er 294 miljard e-mail verstuurt.
6. 89,1% van die e-mail betreft spam, dat zijn 262 miljard e-mails.
7. Al die e-mails worden verstuurd door 1,88 miljard e-mail gebruikers.
8. 25% van die e-mail gebruikers zakelijk zijn.
9. 12% Van de websites zijn pornografisch.
10. Cybercriminaliteit kost de samenleving 10 miljard per jaar.
11. Wereldwijd maken 26,6% van de mensen gebruik van het internet.
12. In Europa maken 50,3% gebruik van het internet.
13. Elke minuut wordt er voor 48 uren aan video's geüpload op Youtube.
14. Dat zijn 8 jaren aan video's per dag.
15. Ook worden er 3 miljard video's per dag bekeken op Youtube.
16. Er zijn nu ongeveer 1,5 miljoen .be domeinnamen geregistreerd bij DNS.be.
17. In 2010 waren er 202 miljoen geregistreerde domeinnamen in totaal.
18. Elke dag worden er 50 miljard Tweets de wereld ingestuurd.
19. Dan zijn 600 Tweets per seconden!
20. Hyves heeft ondanks Facebook nog steeds bijna 11 miljoen leden.
21. Facebook heeft 800 miljoen actieve gebruikers.
22. Er zijn ongeveer 7.000 domeinnamen met de extensie .vlaanderen geregistreerd bij DNS.be.
23. Wereldwijd hebben 2 miljoen bedrijven een bedrijfspagina