

CCV centrum voor criminaliteitspreventie en veiligheid

Cybercrime bijeenkomsten

Ideeënhandboek voor PVO's

Ministerie van Justitie en Veiligheid

PVO

MKB Nederland

Detailhandel Nederland

Inhoudsopgave

1. Inleiding **3**

2. Publiekscampagne **4**
2.1 Inhoud campagne 4
2.2 Phishing 4
2.3 Veiliginternetten.nl 4
2.4 Communicatiemiddelen 4
2.5 Start campagne 5
2.6 Meedoen aan de campagne 5

3. Trainingen **7**
3.1 Organisatie 7
3.2 Programma 7
3.3 Locatie 8
3.4 Trainers 8

4. Congressen **13**
4.1 Organisatie 13
4.2 Locatie en datum 13
4.3 Programma 13
4.4 Spreker 14
4.5 Workshops 14
4.6 Promotie 14

5. Promotiemateriaal **23**
5.1 Uitnodiging 23
5.2 Filmpje met praktijkverhalen 23
5.3 Phishing klapper 23

6. Hulp bij organisatie **24**

7. Checklist **25**

Centrum voor Criminaliteitspreventie en Veiligheid
versie 2019.01

1. Inleiding

Cybercrime is helaas voor veel ondernemers een toenemend probleem. Uit onderzoek blijkt dat 1 op de 5 mkb-bedrijven ermee te maken krijgt. De meest voorkomende vormen van cybercrime zijn ransomware, phishing, identiteitsfraude en oplichting. De schade bij een cyberincident kan groot zijn. Denk alleen al aan de kosten voor herstel of vervanging van de website, programma's of data, maar ook omzetverlies en reputatieschade.

Het ministerie van Justitie en Veiligheid wil mkb-bedrijven weerbaarder maken tegen cybercrime. Hiervoor is subsidie beschikbaar gesteld aan alle PVO's voor het organiseren van voorlichtingsbijeenkomsten over cybercrime voor ondernemers en hun medewerkers.

Het CCV en sommige PVO's hebben al ervaring met de organisatie van dergelijke bijeenkomsten. Het CCV heeft de beschikbare kennis gebundeld in dit ideeënhandboek zodat alle PVO's hiervan gebruik kunnen maken.

Als zich in de loop van de subsidieperiode nieuwe ideeën aandienen, worden deze toegevoegd in het handboek.

Mogelijk gemaakt door: Ministerie van Justitie en Veiligheid

In samenwerking met: MKB Nederland, Detailhandel Nederland

2. Publiekscampagne ‘Eerst checken, dan klikken’

Als onderdeel van de integrale aanpak van cybercriminaliteit investeert het ministerie van Justitie en Veiligheid onder andere in preventie. Dit wordt onder meer uitgewerkt in de vorm van een landelijke publiekscampagne.

2.1 Inhoud campagne

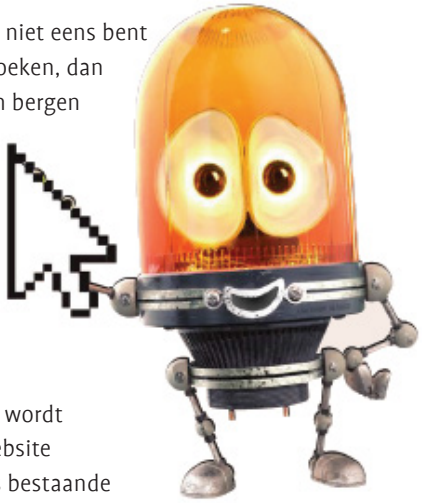
De campagne is gericht op iedere Nederlander die zich op de digitale snelweg begeeft. Het doel van de campagne is iedereen te waarschuwen – doch niet bang te maken – voor de risico’s die je loopt als je je niet veilig online begeeft. Ook mensen die denken dat ze alles online al goed hebben geregeld; dat is namelijk niet altijd zo. Het gaat in de campagne niet alleen om waarschuwen. Ook worden vijf basistips gegeven die iedere Nederlander ter harte zou moeten nemen om het cybercriminelen niet te makkelijk te maken.

De vijf basistips zijn afkomstig van een hackerscollectief. Zij hebben aangegeven wat de grootste kwetsbaarheden zijn bij de gemiddelde Nederlander; hoe zij het gemakkelijkst ‘binnen kunnen dringen’, met alle gevolgen van dien. Deze tips zijn ook besproken met de Consumentenbond, die veel doen aan het waarschuwen van consumenten voor cybercriminelen. De tips luiden:

- eerst checken, dan klikken. Klik niet zomaar op iedere link of bijlage,
- gebruik verschillende sterke wachtwoorden,
- voer software updates altijd direct uit,
- gebruik altijd een virusscanner en
- maak regelmatig een back-up.

2.2 Phishing

De eerste tip is meteen de moeilijkste. En zegt ook veel over hoe iemand zich online gedraagt. Daarom wordt de televisiecommercial gevormd rondom het thema phishing. Iedereen kent ze wel, de mailtjes van de bank waarbij je niet eens bent aangesloten. Of nepbetaalverzoeken, dan wel lokkertjes waarin je gouden bergen worden beloofd. Hierbij moet je alert zijn. En eerst nadenken. Daarom komt de tip: eerst checken, dan klikken terug in de televisiecommercial.



2.3 Veiliginternetten.nl

Wat je eerst moet checken, dat wordt beschreven op de campagnewebsite veiliginternetten.nl. Deze reeds bestaande website besteedt aandacht aan de campagne door tips te geven over hoe je bijvoorbeeld een nepmail kunt herkennen en wat je vervolgens kunt doen. Ook wordt op de website gewezen op de vier andere basistips. Dus: phishing is het overkoepelende thema en zorgt voor bewustwording, de website geeft verdere uitleg.

2.4 Communicatiemiddelen

Naast de televisiecommercial wordt de campagne ook via social media verspreid. Denk aan banners waarin je wordt getest op het herkennen van een nepmailtje. Verschillende ICT-, internet- en telecombedrijven en banken werken mee aan de campagne, onder meer door nepmails die zogenaamd vanuit deze bedrijven zijn verstuurd beschikbaar te stellen voor de banners. Denk aan een nepmail van een bank, waarin iemand wordt gesommeerd een nieuwe betaalpas aan te vragen, en wel binnen een dag. Of vanuit de rijksoverheid, het verzoek om met DigiD in te loggen op mijnoverheid.nl.

Andere uitingen betreffen mediapartnership/branded content, Digital out of Home, PR, influencers, online video, interactive display, online display en contextuele online display.

2.5 Start campagne

De campagne start op 25 mei 2019. Minister Grapperhaus trapt de campagne af tijdens de landelijke veiligheidsdag die in Almere wordt georganiseerd en in het teken staat van cybercrime. Ook de staatssecretaris Keijzer van Economische Zaken en Klimaat is aanwezig, evenals de deelnemende bedrijven die de campagne via eigen kanalen zullen verspreiden. De campagne zal in het najaar 2019 worden herhaald.

2.6 Meedoen aan de campagne

Hoe meer aandacht de campagne krijgt, des te beter. Om die reden is een groot aantal bedrijven en brancheorganisaties reeds aangesloten. Via de website veiliginternetten.nl zal een toolbox beschikbaar worden gesteld. In de toolbox vind je de uitingen van de campagne, de televisiecommercial en de banners, die je kunt inzetten.



3. Trainingen

Een kleinschalige bijeenkomst in de vorm van een training is een goede manier om informatie over te brengen aan ondernemers en hun medewerkers. In de training leren de deelnemers meer over cybercrime en hoe zij zich hiertegen kunnen wapenen. Ze krijgen inzicht in wat er op dit moment speelt bij mkb-bedrijven en horen van collega-ondernemers wat hen is overkomen en wat daarvan de gevolgen zijn geweest. In de training krijgen ze praktische preventietips die ze direct kunnen toepassen. Daarbij gaat het niet per se over ingewikkelde technische oplossingen, maar vooral over eenvoudig te nemen maatregelen en het eigen gedrag om de digitale veiligheid te verbeteren.

3.1 Organisatie

De training wordt vaak georganiseerd in samenwerking met de gemeentes waar de training wordt gehouden. Zij hebben lokaal goede contacten, bijvoorbeeld voor het regelen van een locatie en de catering. Bovendien beschikken gemeentes over de contactgegevens van alle bedrijven en kunnen zij hun communicatiekanalen inzetten om de bedrijven te bereiken. Denk aan een uitnodiging per mail of per post, een aankondiging op de website, de gemeentepagina in huis-aan-huisbladen, de inzet van sociale media en een persbericht. Schakel ook altijd de hulp in van ondernemersverenigingen en de lokale MKB-afdelingen om de doelgroep te bereiken.



Blijft het aantal aanmeldingen achter? Dan is een flyeractie een goede optie. Ga persoonlijk langs bij de bedrijven en nodig ze uit. Vraag hierbij om ondersteuning van een boa of wijkagent.

3.2 Programma

Om zoveel mogelijk deelnemers te bereiken kan de training het beste in de avond worden gehouden, buiten kantooruren en na sluitingstijd van de meeste winkels. Een aftrap door de burgemeester onderstreept het belang van de training.

Een avondprogramma kan er als volgt uitzien:

17:45 uur	Inloop met een broodje
18:30 uur	Welkom door burgemeester
18:45 uur	Training ‘Digitaal Veilig’
20:15 uur	Napraten met een drankje
20:45 uur	Einde bijeenkomst



Organiseer eens een ochtendsessie in de vorm van een cyberontbijt. Een goed begin van de dag. De deelnemers kunnen de tips van de training tijdens hun werkdag direct in de praktijk brengen.

Zorg tijdens de inloop minimaal voor een broodje en eventueel soep of een warm gerecht, zodat de deelnemers niet eerst naar huis hoeven om te eten. Na afloop kun je nog een drankje aanbieden, zodat er nog even gelegenheid is om na te praten.

De training zelf duurt ongeveer 1,5 uur. Dat is lang genoeg om de basiskennis over te brengen en kort genoeg om de aandacht van de deelnemers vast te houden.

Het programma kan naar wens worden uitgebreid met bijvoorbeeld een korte presentatie van de politie over hun rol bij cybercrime.

Een andere optie is om deelnemers tijdens het napraten de gelegenheid te bieden om (persoonlijke) vragen over online beveiliging te stellen aan de trainer. Of ga hiervoor een samenwerking aan met IT-studenten.

3.3 Locatie

De training wordt bij voorkeur georganiseerd op een aansprekende locatie, die goed bereikbaar is. Belangrijk is dat de locatie voorziet in genoeg plek voor het gewenste aantal deelnemers. Voor de trainingen wordt uitgegaan van gemiddeld 50 deelnemers. Denk ook aan de zaalopstelling, de catering, audiovisuele middelen en eventueel technische ondersteuning.

3.4 Trainers

Er zijn genoeg cyberexperts die trainingen kunnen geven. Het belangrijkste criterium is dat zij in staat zijn om de kennis goed over te brengen op de doelgroep mkb-ondernemers en hun medewerkers. Op de volgende pagina's vind je informatie over trainingsbureaus en zelfstandige trainers die dit soort trainingen vaker hebben gegeven en landelijk ingezet kunnen worden.



Wil je ondersteuning bij het boeken van een trainer, het aanmelden van de deelnemers of het promotiemateriaal, zoals de uitnodiging of een persbericht? Neem contact op met het CCV secretariaat Lokale Veiligheid, telefoon 030 751 67 99 of e-mail lokaleveiligheid@hetccv.nl.

Trainer: Wouter van Dongen



Wouter is een ervaren securityspecialist/ethisch hacker met ruim 15 jaar ervaring in het IT-security vakgebied en is naast beveiligingsexpert eveneens webontwikkelaar. Naast behaalde Certified Information Systems Security Professional en Certified Information Systems Auditor certificeringen, is Wouter meerdere malen in de media geweest met betrekking tot geconstateerde beveiligingslekken en issues bij grote bedrijven, banken en publieke instanties. Ook wist hij zich als beveiligingsonderzoeker binnen een jaar in de Top 10 wereldwijd te vestigen van bug bounty platform Bugcrowd.

DongIT

Wouter is directeur van DongIT, een IT-bedrijf dat webapplicaties en webinfrastructuren ontwikkelt, beveiligt en beheert. Daarnaast voeren zij beveiligingsassessments (pentesten) uit op webapplicaties en -infrastructuren.

Wat kun je verwachten?

Gedurende de presentaties zal Wouter enkele voorbeelden van hacks aanhalen door middel van verhalen en divers beeldmateriaal. Om te voorkomen dat de aandacht van het publiek verslapt of dat de inhoud te complex wordt, zal er geen live hackdemonstratie gegeven worden. Door middel van vooraf geprepareerde filmpjes zal gedemonstreerd worden hoe een hacker te werk gaat en hoe websites mogelijk gemanipuleerd en bezoekers misleid kunnen worden. Verder passeren tijdens de presentaties o.a. de volgende onderwerpen de revue:

- Wouter vertelt vanuit eigen ervaringen en uitgevoerde hacks in het verleden, variërend van onschuldige en grappige hacks bij studentenverenigingen tot hackaanvallen die hebben geleid tot rechtszaken en het halsoverkop moeten vluchten uit Curaçao.
- Wat is de ‘denkwijze’ van een hacker? Hoe gaat een hacker te werk? Waarop focust een hacker zich als hij/zij een bedrijf wil hacken? Bijvoorbeeld een open bronnen onderzoek: welke informatie is er online te vinden over een bedrijf? Welke informatie slingert er rond op het internet wat gebruikt kan worden voor een hackaanval?
- Tips & tricks: waar moeten mkb-ondernemers op letten, wat zijn ‘eenvoudige’ manieren om te voorkomen dat het bedrijf wordt gehackt en de beveiliging sterker te maken. Bijvoorbeeld een sterk wachtwoordbeleid, implementatie van een responsible disclosure beleid, beveiligingseisen stellen aan developers, etc.

Prijsindicatie:	€ 1.250,- excl. btw (mede afhankelijk van het aantal trainingen)
Meer info:	DongIT Telefoon: 071 52 49 213 E-mail: info@dongit.nl www.dongit.nl

Trainer: Luc Pluimakers



Luc Pluimakers is een 19-jarige enthousiaste wizzkid, die naast zijn studie Information Security Management aan de Haagse Hogeschool ook in dienst is bij NFIR BV. Core-business van NFIR is incident response en forensisch onderzoek. Ook wel genoemd: de digitale brandweer met veel ervaring met bedrijven die gehackt zijn en waarom en hoe ze gehackt zijn. Deze ervaringen gebruikt Luc tijdens zijn presentaties met praktische, meeslepende en interactieve voorbeelden. Hij gebruikt zijn leeftijd om zijn toehoorders te laten inzien dat die jongen op de zolderkamer echt een gevaar kan zijn. Luc heeft ervaring en kennis als het gaat over de sociale kant van het hacken.

Wat kun je verwachten?

In de trainingen geeft Luc Pluimakers, als jonge hacker in combinatie met de kennis van NFIR, inzichten in wat hackers doen en wat de risico's zijn voor mkb-bedrijven. De presentatie is zeer interactief en zal de aanwezigen meeslepen om mee te discussiëren over de gevaren die men loopt en de oplossingen die er zijn voor deze gevaren. In een presentatie van 1 tot 1,5 uur neemt Luc de deelnemers mee in een bewustwordingsproces.

Na afloop van de training krijgen de deelnemers de mogelijkheid om zich te laten helpen door aanwezige IT studenten. Per 20 aanmeldingen zorgt NFIR voor 1 student. Vragen over twee-staps-authenticatie, password managers, sterke wachtwoorden, social media instellingen etc. zullen worden beantwoord en indien mogelijk helpen de studenten ook direct bij het instellen. Alle studenten zijn in dienst van NFIR BV en hebben allemaal Korpschef goedkeuring.

Deze werkwijze maakt de training zeer interactief, leerzaam en laagdrempelig voor iedereen. Een bewustwordingspresentatie waarna iedereen weet dat ontkenning van de ernst van het onderwerp geen optie meer is, en dat oplossingen eenvoudig te realiseren zijn.

Prijsindicatie:	€ 1.000,- excl. btw (inclusief de kosten van studenten en reiskosten)
Meer info:	NFIR BV Telefoon: 088 323 02 05 / 06 43 45 66 40 E-mail: l.pluimakers@nfir.nl www.nfir.nl

Trainer: Stan Hegt



Stan is een goedaardige hacker. Wat begon als hobby op tienjarige leeftijd, groeide al snel uit tot zijn werk. In zijn dagelijkse leven werkt Stan voor Outflank, een security bedrijf dat Stan met andere tophackers heeft opgericht en welke zich bezighoudt met geavanceerde aanvalstesten en het beperken van de schade bij digitale inbraken. Als test en uitsluitend op verzoek van zijn klanten, heeft Stan bij allerlei organisaties digitaal ingebroken: van oliebedrijven tot banken en overheidsorganisaties. Hij deelt graag zijn ervaringen over hoe je kwaadwillende hackers buiten de deur kunt houden.

Wat kun je verwachten?

Tijdens deze presentatie gaat Stan in op de actuele ontwikkelingen van cyberdreigingen en legt hij uit op welke wijze hackers te werk gaan. Aan de hand van praktische voorbeelden en live demonstraties laat hij zien hoe cybercriminelen bij organisaties en burgers proberen in te breken. Bovendien laat Stan zien wat je zelf kunt doen om je eigen computer en je bedrijf beter te beschermen tegen digitale aanvallen. Hiervoor hoef je absoluut geen computerexpert te zijn.

Aan bod komen onder andere:

- Waarom ben je wel of niet interessant voor hackers?
- Hoe gaan cybercriminelen te werk?
- Live demo's van cybercrime aanvallen om de risico's beter te kunnen begrijpen.
- De belangrijkste maatregelen om de risico's van digitale inbraken te beperken.

Prijsindicatie:	€ 1.450,- excl. btw
Meer info:	Stan Hegt
	Telefoon: 06 11 88 50 39
	E-mail: info@stanhegt.nl
	www.stanhegt.nl


CCV
Veiligheid maken we samen
Wie is nou die internetcrimineel?
APT28

4. Congressen

Om het belang van cybercrimepreventie in jouw PVO regio te onderstrepen, kun je uitpakken met een congres. Het is tevens een goede manier om jouw PVO op de kaart te zetten. Zo bied je ook ondernemers uit gemeentes waar geen training is georganiseerd, de kans om zich te verdiepen in het onderwerp.

4.1 Organisatie

Er komt nogal wat kijken bij de organisatie van een congres. Het is verstandig om een werkgroepje samen te stellen die de organisatie op zich neemt. Betrek ook de gemeente waar het congres wordt gehouden bij de werkgroep. Als gastgemeente hebben zij er ook belang bij dat het congres goed wordt neergezet. De organisatie van een congres kost meer tijd dan je denkt. Een optie is om de hulp van een congresbureau in te schakelen die de organisatorische werkzaamheden op zich kan nemen.



Begin tijdig met de voorbereiding. Locaties en sprekers zijn vaak ver van tevoren al volgeboekt. Houd rekening met minimaal 4-6 maanden voorbereidingstijd.

4.2 Locatie en datum

Het begint bij het bepalen van een goede locatie voor het congres. Een van de belangrijkste factoren bij het uitzoeken van een locatie is de centrale ligging en de bereikbaarheid. Naast voldoende en/of gratis parkeergelegenheid is ook de bereikbaarheid met de auto of het ov belangrijk. Natuurlijk moet de locatie voldoende ruimte bieden voor het aantal deelnemers. Voor een congres wordt uitgegaan van 100 - 150 deelnemers. Kijk of de plenaire zaal aangepast kan worden aan het uiteindelijke aantal deelnemers, dus groter of kleiner gemaakt kan worden. Check ook of er aparte ruimtes beschikbaar zijn voor eventuele workshops of subsessies.

Ook de datum kan bepalend zijn voor het slagen van een congres. De beste (en drukste) congresmaanden zijn maart, april, juni, september en oktober. Over het algemeen zijn dinsdag en donderdag de beste dagen waarop deelnemers kunnen.



Controleer of de geplande datum niet op een feestdag, een dag met een landelijk evenement (voetbal), Prinsjesdag, of een vakantiedag valt. Check de vakanties op www.rijksoverheid.nl/onderwerpen/schoolvakanties.

4.3 Programma

De avond lijkt het meest geschikte tijdstip voor de doelgroep, na sluitingstijd van de winkels en andere mkb-bedrijven.

Een avondprogramma kan er als volgt uitzien:

18:00 uur	Inloop met een warm buffet
19.00 uur	Plenaire opening met hoofdspreker
20.00 uur	Einde plenaire opening, naar de workshops
20 10 uur	Start workshop 1 (drankjes in de zaal)
20.55 uur	Naar de volgende workshop
21.00 uur	Start workshop 2 (drankjes in de zaal)
21.45 uur	Plenaire afsluiting
22.00 uur	Start borrel

Zorg voor een ervaren avondvoorzitter die het programma op een leuke manier aan elkaar kan praten en de tijd bewaakt.

Het avondprogramma duurt te lang als u tussentijds nog een pauze inplant. Zorg daarom dat er tijdens de workshops drankjes in de zaal aanwezig zijn.



Je kunt natuurlijk ook overwegen om het congres aan het einde van de middag te laten beginnen. Mkb-ondernemers met meerdere medewerkers kunnen vaak wel een paar uurtjes eerder weg. Start dan met de hoofdspreker, gevolgd door een buffet en sluit af met de workshops.

4.4 Spreker

Een goede hoofdspreker is een vereiste om voldoende deelnemers aan te trekken. Je kunt bijvoorbeeld kiezen voor een bekende Nederlander als misdaadjournalist Peter R. de Vries, een bekende hacker of schrijvers die spraakmakende lezingen geven over het onderwerp cybercrime. De spreker moet in ieder geval het publiek weten te inspireren met zijn of haar verhaal en in staat zijn om het taalgebruik en de toon aan te passen aan de doelgroep. Op de volgende pagina's vind je een selectie van ervaren sprekers die je kunt inzetten voor het congres.

4.5 Workshops

Zorg voor wat interactieve workshops in het programma. Zo bied je deelnemers de mogelijkheid om in kleinere groepen wat meer kennis op te doen over een specifiek onderwerp dat hun interesse heeft. Verderop in dit boekje vind je enkele voorbeelden van workshops.

4.6 Promotie

Er zijn verschillende manieren om de bijeenkomst te promoten:

- Zorg voor een aansprekende uitnodiging. Een digitale uitnodiging is makkelijk te verspreiden. Verstuur de uitnodiging uiterlijk 4-6 weken van tevoren. Daarna kun je nog één keer een herinnering sturen.



Stuur ongeveer 2-3 maanden van tevoren een 'Save the date' mail. In deze mail hoef je nog geen gedetailleerde informatie over het programma te vermelden, alleen de datum en de locatie. Het doel is om de ontvangers nieuwsgierig te maken over een evenement dat ze niet mogen missen!

- Je kunt ook alle netwerkpartners, zoals MKB-Nederland en Detailhandel Nederland en de gemeentes en ondernemersverenigingen in jouw regio vragen om de digitale uitnodiging door te sturen naar hun achterban. Zo creëer je een groot bereik. Laat ook wat uitnodigingskaarten drukken, zodat je die kunt uitdelen tijdens andere bijeenkomsten waar de doelgroep aanwezig is.



Maak een speciale hashtag voor het congres en gebruik die in alle berichten die je op social media plaatst. Zo creëer je veel aandacht voor jouw evenement.

- Stuur een persbericht naar de lokale en regionale media en nodig ze uit voor het congres. Hoe groter de media-aandacht, hoe meer ondernemers je bereikt met de boodschap.
- Gebruik je eigen communicatiekanalen om het congres onder de aandacht te brengen. Plaats berichten in de nieuwsbrief, op de PVO-website, Twitter, Facebook en andere social media. Vraag andere partijen, zoals MKB-Nederland, Detailhandel Nederland, gemeentes en ondernemersverenigingen, hetzelfde te doen.

Spreker: Maria Genova



Maria Genova wordt geboren op 12 januari 1973 in het Bulgaarse Plovdiv. Na afronden van het gymnasium volgt ze haar Nederlandse man op negentienjarige leeftijd naar zijn geboorteland. Al van kleins af aan is het haar droom om journalist te worden, maar hoe word je dat in een vreemd land? Met een beetje geluk en heel veel doorzettingsvermogen lukt het haar om al binnen een jaar als verslaggever voor een regionaal dagblad aan het werk te gaan.

Niet veel later gaat ze studeren aan de Academie voor Journalistiek in Tilburg en werkt ze voor diverse kranten en tijdschriften. In 2007 debuteert ze als auteur met 'Communisme, sex en leugens', een tragikomisch boek over het leven van de gewone mensen tijdens het communisme en over de voor- en de nadelen van een dictatuur. Voor haar debuut ontvangt ze de Looijer Debutantenprijs.

Wat kun je verwachten?

Maria Genova is een vooraanstaand journaliste en schrijfster die bekend staat om haar spraakmakende boeken en lezingen.

'Communisme, sex en leugens' zou niet het laatste boek van Maria Genova zijn. Later volgen titels als 'Man is stoer, vrouw is hoer' (over loverboys en vrouwenhandel in Nederland – een absolute bestseller), 'Vrouwen te koop' en 'Het Duivelskind'. Laatstgenoemde boek haalt ondanks de zware onderwerpen (kindermishandeling en falende jeugdzorg) zowel de Nederlandse als de Belgische bestsellerlijsten.

De auteur breidt haar bibliografie vervolgens uit met een titel over een totaal ander speelveld – ict, hackers en identiteitsfraude. Als digibeet presteert ze het om met 'Komt een vrouw bij de h@cker' een grote hit te scoren in het bedrijfsleven. Sindsdien is ze uitgegroeid tot specialist in dit onderwerp en wordt ze veel gevraagd voor lezingen tijdens een congres of presentaties. Deze breed onderlegde persoonlijkheid maakt haar presentaties voor opdrachtgevers altijd op maat.

Prijsindicatie:	Vanaf € 1.000,- excl. btw
Meer info:	www.mariagenova.nl
	www.quality-bookings.nl

Spreker: Dave Maasland



Dave Maasland (1990) is CEO bij ESET Nederland. Dit is één van de grootste IT-Security bedrijven van Nederland en het merk ESET is wereldwijd vertegenwoordigd.
Maasland: “IT en technologie zijn echt een passie van mij en het raakt me dat mensen daar angst voor hebben. Het belang van IT wordt nog steeds onderschat, daar ligt onze meerwaarde. Zelf kreeg ik mijn eerste computer op mijn zesde en maakte al snel kennis met het fenomeen ‘virus’. Gelukkig hebben we daar inmiddels goede software voor om dat te voorkomen. Met ruim 100 miljoen gebruikers beschikken we over veel data en steeds meer kennis, die we gebruiken om steeds een stapje voor te blijven. Techniek ontwikkelt zich iedere dag en kan ons nog ontzettend veel mooie dingen brengen.”

Wat kun je verwachten?

Vanuit zijn vakgebied cybersecurity spreekt hij over de risico’s, maar vooral mogelijkheden die de digitale wereld biedt. Met zijn passie voor IT en technologie wil hij mensen enthousiasmeren en angst door onwetendheid wegnemen.

- De Cybercrime Ondernemer
  Deze sessie zoemt in op het verdienmodel van cybercriminelen. Hoe werkt malware en hoe verdient men hier geld mee? En om wat voor bedragen gaat dit dan? Wanneer men de ondernemende kant van cybercrime snapt kan men pas echt begrijpen hoe groot en intens deze wereld is.
- Word Hacker in een half uur
  Iedereen kan hacken alleen is men zich hier nog niet van bewust. Wanneer u weet hoe de aanvaller werkt, is het mogelijk een gedegen verdedigingstactiek op te stellen. Deze presentatie is een ontwapenend verhaal over cybercriminelen en hun tactieken en geeft inzicht in hoe u vandaag nog kunt starten met het creëren van een veiligere digitale werkomgeving binnen uw organisatie. Dit verhaal is voor iedereen geschikt, ook als u niet technisch bent.
- De impact van cybercrime
  Deze presentatie gaart dieper in op de impact van cybercrime op organisaties en de economie in Nederland. Wat merken we als land, bedrijf en individu van cybercrime en wat kunnen we verwachten de komende jaren. En sterker nog, gaan we dit gevecht ooit winnen?

Prijsindicatie:	Vanaf € 2.000,- excl. btw
Meer info:	www.quality-bookings.nl

Spreker: Rickey Gevers



Van vermeend cybercrimineel tot cybersecurity expert. Die verrassende weg legde Rickey Gevers af. Hij begon zijn loopbaan als selfmade hacker, kwam in botsing met het gezag, beterde zijn leven, en is nu een autoriteit op het gebied van internetbeveiliging.
Hij had nooit kwaad in de zin toen hij zich als puber bekwaamde in het hacken van computers. Het ging Rickey Gevers niet om de 'inbraak' zelf, maar om de technische uitdaging. Dat neemt niet weg dat hij in 2008 door de politie van zijn bed werd gelicht. Hij had de server van de Universiteit van Michigan gehackt. De FBI kwam zijn IP-adres op het spoor en tipte de Nederlandse politie. Gevers belandde in de cel. In 2011 kreeg hij een voorwaardelijke straf. Maar niet voordat hij beterschap beloofde.

Heel Nederland leerde deze spreker kennen toen hij in 2013 het Pobelka Botnet ontdekte, dat het bedrijfsleven dreigde plat te leggen. Als presentator van het 3Lab-programma Hackers maakte hij inzichtelijk hoe computercriminelen te werk gaan.

Wat kun je verwachten?

Cybersecurity is een actueel vraagstuk. Bedrijven investeren kapitalen in de beveiliging van hun systemen en gegevens. Toch komen er om de haverklap gevoelige data op straat te liggen. Het is een kat-en-muis-spel tussen security experts en hackers. Spreker Rickey Gevers was zo'n hacker, maar staat nu aan de goede kant van de streep. Gevers weet precies hoe het kraken van computercodes in zijn werk gaat. Als puber deed hij niet anders. 'Gewoon voor de lol'. Nu zet hij zijn ervaring in om bedrijven en overheden te helpen hun beveiliging te optimaliseren.

Wil je tijdens het congres kennis delen over de gevolgen van een hack en een discussie initiëren over hoe bedrijven daarmee om kunnen gaan en hoe datalekken te voorkomen zijn? Met Rickey Gevers haal je een 'echte hacker' in huis, die zich ontwikkelde tot security expert met buitengewoon veel kennis van 'incident response'. Hoe zijn hacks te voorkomen? Wat doe je als bedrijf als een hack de dagelijkse business in gevaar brengt?

Prijsindicatie:	Vanaf € 2.000,- excl. btw
Meer info:	Informeer bij een boekingsbureau

Spreker: Dick Berlijn



Dick Berlijn (1950) is een telg uit een luchtmachtfamilie. Zijn vader, die jachtvlieger en commandant van het Commando Tactische Luchtstrijdkrachten van de Luchtmacht was, strekte hem tot voorbeeld. Berlijn genoot zijn opleiding aan de Koninklijke Militaire Academie in Breda. Zijn opleiding tot militair vliegenier rondde hij in 1975 af in Canada. Ook doorliep hij een opleiding tot wapeninstructeur.

Berlijn maakt een indrukwekkende loopbaan bij defensie, die begint als Operationeel Officier en Hoofd van de Transitie en Conversie Afdeling op vliegbasis Leeuwarden. Hij heeft ingrijpende en succesvolle transities in de boeken staan. In Denemarken is Berlijn enige tijd actief als trainer en instructeur. In 1988 stapt hij over naar het Commando Tactische Luchtstrijdkrachten.
Als geboren leider doorloopt Berlijn diverse stevige opleidingen en voert het commando over uiteenlopende militaire vliegbases en operaties. In 1993 houdt hij als eerste commandant toezicht op het vliegverbod boven Servië. Hij speelt een rol bij diverse UNIFIL-operaties en dient in de Afghaanse oorlog.

Wat kun je verwachten?

Cybersecurity, openbare orde en veiligheid, leiderschaps-vraagstukken. Het zijn thema's die spreker Dick Berlijn nauw aan het hart gaan. De bekende generaal buiten dienst der Nederlandse strijdkrachten volgt de actualiteit op de voet en weet zijn expertise in genoemde onderwerpen als spreker met passie voor het voetlicht te brengen.

Van oorlog in real life naar oorlog in cyberspace. Het lijkt een grote stap, maar dat is het absoluut niet. Want de echte oorlog wordt allang niet meer alleen gevoerd met mitrailleurs, kernwapens en tanks, weet Dick Berlijn. Of we in oorlog zijn? "Een lastige vraag", zegt Dick Berlijn, cybersecurity expert. "Dat hangt ervan af wat je onder oorlog verstaat." Volgens de voormalig Commandant der Strijdkrachten is het antwoord in de klassieke zin van het woord oorlog een duidelijk nee. We zijn niet letterlijk in oorlog, land tegen land. "Maar dat betekent niet dat cybercrime niet heel veel schade aanricht. En dat betekent ook niet dat er geen landen zijn die andere landen aanvallen. Er zijn staten die heimelijke acties uitvoeren die het functioneren van andere landen ondermijnen. En dat zorgt voor heel veel problemen."

Met kennis van zaken en een directe, aansprekende stijl als spreker voegt oud-militair Dick Berlijn waarde toe aan een congres. Hij bereidt zijn lezingen en presentaties minutieus voor en legt gemakkelijk verbindingen met kleine en grote gezelschappen.

Prijsindicatie:	Prijs op aanvraag
Meer info:	www.quality-bookings.nl

Spreker: Brenno de Winter



Brenno de Winter (1971) begon in de automatisering. Hij schreef onder meer bedrijfssoftware. Zijn nieuwsgierige en kritische aard maakte dat hij in 2000 overstapte naar de onderzoeksjournalistiek. Hij geldt als absolute autoriteit op het gebied van cybersecurity en internet-privacy. De Winter schrijft onder meer voor nu.nl en diverse vaktijdschriften en heeft meerdere boeken op zijn naam staan. Hij onderzocht meer dan tweeduizend datalekken en werd in 2011 uitgeroepen tot journalist van het jaar. Hij zal voor altijd de boeken ingaan als de onderzoeksjournalist die het lek in de OV-chipkaart aantoonde, wat hem door de overheid niet in dank werd afgenomen.

Als auteur schreef hij daarnaast diverse boeken, waaronder een roman, getiteld de Rode Hack. Zijn non-fictieboek Digitale Stormvloed wordt vaak genoemd als 'verplichte literatuur' voor bestuurders en bedrijven die inzicht willen hebben in de kansen en bedreigingen van internet.

Wat kun je verwachten?

In een steeds verder digitaliserende wereld zijn cybersecurity en privacy urgente thema's. Ieder bedrijf en elke organisatie heeft ermee te maken. Als spreker weet Brenno de Winter als geen ander inzicht te bieden in zowel de kansen als zwakke plekken in ICT en automatisering.

Hoe voorkom je hacks? Hoe beperk je de schade van datalekken? Hoe bied je privacygaranties? Van digitalisering tot cybercrime en informatiebeveiliging, het is het domein van Brenno de Winter. Als spreker legt hij de zwakke plekken bloot, met indringende presentaties en zelfs met een interactieve serious game.

Prijsindicatie:	Vanaf € 2.000,- excl. btw
Meer info:	www.dewinter.com
	of informeer bij een boekingsbureau

Spreker Peter R de Vries



Peter R(udolf) de Vries begint zijn journalistieke loopbaan in 1978 op de Haagse redactie van De Telegraaf. Daar groeit al snel zijn interesse en voorliefde voor misdaadverslaggeving. In 1987 wordt De Vries hoofdredacteur van het weekblad Actueel, dat hij vervolgens omvormt tot een misdaadmagazine. Vanaf 1991 heeft De Vries een eigen bureau in misdaadverslaggeving en schrijft hij columns voor week- en dagbladen. Daarnaast is hij auteur van een aantal goed verkopende misdaadboeken, waaronder een publicatie over de Heineken-ontvoering.

Wat kun je verwachten?

Met Peter R. de Vries haal je een bekende televisiepersoonlijkheid en kleurrijk spreker in huis. Hij is bedenker en eindredacteur van onder meer het misdaadprogramma Crime-Time, en presentator, bedenker en hoofdredacteur van het televisieprogramma Peter R. de Vries, misdaadverslaggever, dat na vele succesvolle jaren in 2012 voor het laatst te zien is. De Vries houdt zich bezig met geruchtmakende zaken als de Baarnse moordzaak, de Schiedammer parkmoord, de Puttense moordzaak en de verdwijning van Natalee Holloway. Een uitzending over Natalee Holloway levert hem een Emmy Award op. In 2003 wordt Peter R. de Vries door omroepblad Broadcast Magazine uitgeroepen tot Omroepman van het Jaar.

Tijdens zijn kleurrijke carrière heeft misdaadverslaggever Peter R. de Vries vele criminelen ontmaskerd en tal van zaken aan het licht of nader tot een oplossing gebracht. In zijn veelbekeken, spraakmakende televisieprogramma's en in boeken en artikelen stort hij zich energiek op de misdaad.

Prijsindicatie:	Vanaf € 5.000,- excl. btw
Meer info:	www.peterrdevries.nl
	of informeer bij een boekingsbureau

Spreker: Jesse van Doren



Jesse van Doren (1996) belichaamt de ‘technologie-generatie’. Al op jonge leeftijd richtte hij zijn eigen onderneming op. Zijn studie Small Business & Retail Management brak hij ervoor af. Met zijn passie voor marketing zet Jesse van Doren bedrijven op scherp.

Jesse van Doren adviseert bedrijven op strategisch niveau, werkt mee aan experimenten op de werkvloer, en is initiator van diverse tech-communities in meer dan twintig landen. Met zijn verschillende social media accounts bereikt hij maandelijks meer dan drie miljoen mensen. Zijn netwerk is enorm en geen enkele trend op het gebied van techniek en marketing ontsnapt aan zijn aandacht.

Jesse van Doren werd meerdere keren bekroond tot ‘meest beloftevolle ondernemer’.

Wat kun je verwachten?

Als jonge, innovatieve entrepreneur adviseert hij bedrijven over groei door de implementatie van slimme marketingtechnieken. Zijn unieke visie op techniek en ‘innovatiemarketing’ maakt dat bedrijven hem graag inhuren als spreker.

Besluit je om de succesvolle ondernemer te boeken voor het congres dan haal je een specialist in het ‘Growth Hacking-proces’ in huis, een marketingproces dat wordt gestuurd door hedendaagse data- en monitortechnieken en kleine experimenten. Van Doren hielp al meer dan driehonderd organisaties vooruit door ze in dit proces mee te nemen. In 2014 organiseerde hij de eerste ‘World Hackaton Day’, waarmee hij internationaal furore maakte.

Prijsindicatie:	Vanaf € 2.000,- excl. btw
Meer info:	www.jessevandoren.com
	of informeer bij een boekingsbureau

Workshop: Ontmoet de hacker

Deze workshop van 30 minuten wordt gegeven door één van de hackers van NFIR BV. Hij laat zien hoe de hacker denkt, waar hij naar op zoek is en hoe hij de digitale openstaande deuren en ramen vindt. Ook zal de hacker een echte hack laten zien. Op een ontspannen, leerzame en duidelijke manier praat de hacker de deelnemers bij over de risico's die ze lopen en hoe ze zich kunnen weren. Hij zal duidelijk maken aan de deelnemers dat het begrip "ik ben niet interessant genoeg voor een hacker" niet bestaat.

NFIR

NFIR BV is een toonaangevend Nederlands cybersecurity bedrijf waarvan de medewerkers korpschef toestemming hebben en onder toezicht staan van het ministerie van Justitie en Veiligheid. Tijdens de dagelijkse werkzaamheden sporen ze hackers op en met de rapportages kan aangifte worden gedaan bij de politie of worden rechtszaken gestart.

Prijsindicatie: € 600,- excl. btw
Meer info: NFIR BV
Telefoon: 088 323 02 05
E-mail: info@nfir.nl
www.nfir.nl

Workshop: Phishing, nr 1 fraude in Nederland

Deze workshop wordt gegeven door Luc Pluimakers van NFIR BV. Hij heeft veel kennis over de oplichters achter deze vorm van financiële fraude. Hij weet hoe men te werk gaat en hoe bedrijven deze aanvallen kunnen voorkomen. Gedurende de workshop wordt ingegaan op verschillende soorten van phishing en de manieren die worden toegepast. Uiteraard vertelt hij ook hoe je phishing kunt voorkomen of in ieder geval herkennen. Er worden echte praktijkvoorbeelden gegeven, die op een laagdrempelige manier worden gepresenteerd. Wat deze workshop extra interessant maakt is dat NFIR vaak aanwezig is bij partijen die slachtoffer zijn geworden van dit soort aanvallen en daardoor beschikt over spraakmakende voorbeelden. Daarnaast is NFIR zelf recentelijk op deze manier aangevallen en door eigen onderzoek is het gelukt om te achterhalen wie dit heeft gedaan en is er aangifte gedaan bij Interpol.

NFIR

NFIR BV is een toonaangevend Nederlands cybersecurity bedrijf waarvan de medewerkers korpschef toestemming hebben en onder toezicht staan van het ministerie van Justitie en Veiligheid. Tijdens de dagelijkse werkzaamheden sporen ze hackers op en met de rapportages kan aangifte worden gedaan bij de politie of worden rechtszaken gestart.

Prijsindicatie: € 600,- excl. btw
Meer info: NFIR BV
Telefoon: 088 323 02 05 / 06 43 45 66 40
E-mail: l.pluimakers@nfir.nl
www.nfir.nl

5. Promotiemateriaal

Voor de promotie van de bijeenkomsten kun je diverse communicatiekanalen inzetten. Denk aan social media, een aankondiging op de PVO website, een uitnodiging per mail of een flyeractie waarbij je persoonlijk langsgaat bij de ondernemers. Vergeet ook niet om de lokale media te informeren over de bijeenkomst. Met een nieuwsbericht in de huis-aan-huisbladen of een item op de lokale radio- of televisiezenders bereik je een groot deel van de doelgroep.

Het CCV heeft een aantal promotiematerialen die je kunt inzetten.

5.1 Uitnodiging

Voor de trainingen is een standaard A5 digitale uitnodiging beschikbaar, die voor jouw bijeenkomst op maat kan worden gemaakt. De uitnodiging kan digitaal worden verstuurd per mail. Het is ook handig om een aantal exemplaren te laten drukken en deze te gebruiken voor een flyeractie of op een andere manier te laten verspreiden door bijvoorbeeld ondernemersverenigingen.



5.2 Filmpje met praktijkverhalen

Verhalen van ondernemers die slachtoffer zijn geworden van cybercrime helpen om de doelgroep de ernst en de noodzaak van preventie in te laten zien. Er is een kort filmpje gemaakt waarin twee ondernemers vertellen wat hen is overkomen. Ze zijn beiden getroffen door ransomware, waardoor het hele bedrijfsproces werd platgelegd. Het kostte de eigenaar van het garagebedrijf en het juwliersechtpaar veel tijd en geld voordat ze alles weer op de rit hadden. Ze weten nu hoe belangrijk het is om goede maatregelen te nemen.

Het filmpje kan bijvoorbeeld worden ingezet voor de werving van deelnemers of worden getoond bij de start van de bijeenkomst. Je vindt het filmpje op het YouTube kanaal van het CCV: https://www.youtube.com/watch?v=JY2RFkwDjc8

5.3 Phishing klapper



Phishing mails worden steeds beter. Ze zijn bijna niet van echt te onderscheiden. Daarom heeft het CCV de 'phishing klapper' gemaakt. Aan de hand van de voorbeelden in deze phishing klapper leer je hoe je kunt beoordelen of een e-mail echt of nep is. Ook staan er tips in hoe je cybercrime zoveel mogelijk kunt voorkomen. Deze handige klapper is gemaakt in de vorm van een bureaukalender, zodat je deze makkelijk neer kunt zetten op een centrale plek in het bedrijf. Zo zorg je ervoor dat iedereen binnen het bedrijf snel op de hoogte is.

Het is een handig naslagwerk om mee te geven aan de deelnemers van een cybercrimebijeenkomst. De phishing klappers zijn gratis aan te vragen bij het CCV.

6. Hulp bij organisatie

Heb je nog vragen of wil je ondersteuning bij het boeken van een trainer of spreker of het aanmelden van de deelnemers? Of wil je gebruikmaken van het beschikbare promotiemateriaal?

Neem contact op met het CCV secretariaat Lokale Veiligheid. Zij helpen je graag om de cybercrimebijeenkomsten tot een succes te maken.

Secretariaat Lokale Veiligheid
Telefoon: 030 751 67 99
E-mail: lokaleveiligheid@hetccv.nl

7. Checklist

ORGANISATIE CYBERCRIMEBIJEENKOMST

1. Algemeen
   - Stel een werkgroepje samen. ☐
   - Maak gebruik van een draaiboek. ☐
2. Locatie bespreken
   - Is de locatie aansprekend voor de doelgroep? ☐
   - Is de bereikbaarheid goed? ☐
   - Is er voldoende ruimte voor het aantal deelnemers en bijvoorbeeld deelsessies? ☐
3. Dag en tijdstip vaststellen
   - Bepaal wat voor de doelgroep het meest geschikte tijdstip is. ☐
   - Geen feestdag, voetbalwedstrijd of vakantie? ☐
4. Trainer/spreker/workshop/dagvoorzitter boeken
   - Onderhandel over de prijs. ☐
   - Maak een goede briefing voor de spreker en de dagvoorzitter. ☐
5. Uitnodiging
   - Save the date versturen ☐
   - Uitnodiging versturen ☐
   - Reminder versturen ☐
   - Aanmeldprocedure regelen ☐
6. Promotie
   - Plaats het bericht op je website. ☐
   - Plaats een bericht in je nieuwsbrief. ☐
   - Zet berichten klaar om te versturen via social media. ☐
   - Stuur informatie over de bijeenkomst naar MKB-Nederland, Detailhandel Nederland, de gemeenten en ondernemersverenigingen in je regio met het verzoek dit verder te verspreiden. ☐
   - Stuur een persbericht naar alle lokale en regionale media en nodig ze uit. ☐

ORGANISATIE CYBERCRIMEBIJEENKOMST

7. Faciliteiten op locatie

- [ ] Maak afspraken over de catering (ontvangst, buffet, pauze en borrel).
- [ ] Zorg voor audiovisuele middelen (in overleg met de sprekers/trainers).
- [ ] Maak afspraken over technische ondersteuning.
- [ ] Bepaal de zaalopstelling.
- [ ] Zorg voor voldoende mensen voor de ontvangst.
- [ ] Regel naambadges (indien gewenst).
- [ ] Huur een eigen fotograaf in.

8. Pers

- [ ] Stel vast wie de pers te woord staat.
- [ ] Stuur achteraf nog een persbericht met foto naar lokale en regionale media.

9. Na afloop van de bijeenkomst

- [ ] Zorg voor een kleine attentie voor de spreker.
- [ ] Deel evaluatieformulieren uit aan de deelnemers.
- [ ] Zorg voor een give-away voor de deelnemers.

10. Evaluatie

- [ ] Evalueer de bijeenkomst. Wat ging er goed? Wat kan beter?

CCV **centrum** voor **criminaliteitspreventie** en **veiligheid**

Het CCV is een onafhankelijke stichting die partijen en veiligheidsprofessionals helpt om Nederland veiliger en leefbaarder te maken.

Churchilllaan 11, 3527 GV Utrecht
Postbus 14069, 3508 SC Utrecht

T (030) 751 67 00
E info@hetccv.nl
I www.hetccv.nl



