Veilig internetten.nl

ALERT online

Allemaal, veilig digitaal!

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

“Wens ons gedoe toe!”

De afgelopen periode heb ik veel collega’s gesproken over de phishing-campagne binnen VenJ. Naast mijn eigen gesprekken, hoorde ik ook de reacties om mij heen. De ene collega vond het een goede actie en de ander vond de hele campagne ronduit belachelijk en veel gedoe. Mooi! Phishing is onderwerp van gesprek en de campagne leeft. Dat was ook precies het doel van deze campagne. Geen stelsel waarin alleen ‘wordt gecontroleerd’ of er goed en bewust met digitaal werken wordt omgegaan of een woud aan bureaucratische regeltjes waar we allemaal een hekel aan hebben. Maar het gezamenlijk hebben over de omgeving waarin wij allen werken. Een omgeving met risico’s die wij niet allemaal kunnen voorzien, maar waar we wel een gezamenlijke verantwoordelijkheid in hebben om ons daar bewust van te zijn. Een omgeving waarin we bewuste keuzes maken. Zoals jaren geleden een collega in het buitenland de bewuste keuze maakte om een gevoelig dossier over een niet beveiligde lijn te versturen, omdat het niet versturen van het dossier de hele operatie in gevaar bracht. Elke keer weer de afweging maken wat is nu van belang, welke risico’s zijn er, welke hulpmiddelen heb ik tot mijn beschikking, welke keuze maak ik, en kan en wil ik deze ook uitleggen.

Dit magazine geeft tips en trucks om phishing te herkennen en vervolgens te voorkomen. Niet alleen als persoon en medewerker, maar ook als projectleider. Want misschien is jouw project of product morgen wel het kanaal waarmee phishing wordt gepleegd. Niet dat phishing het enige risico is waar we mee te maken hebben, maar wel één waar we de hele dag door mee geconfronteerd kunnen worden (zowel zakelijk als privé)!

Geert-Jan van de Ven
CIO Openbaar Ministerie
Voorzitter CISO-board VenJ

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Phishing via smartphone of tablet

Mobiele malware verschilt niet veel met malware voor computers en laptops. Voor cybercriminelen zijn het manieren om persoonlijke gegevens te ontfutselen of kwaadaardige software te installeren. Met als doel om bijvoorbeeld identiteitsfraude te plegen of geld van je bankrekening af te schrijven. Mobiele malware wordt onder andere verspreid via e-mail, sms, WhatsApp en links op websites. Het hengelen naar persoonlijke gegevens wordt phishing genoemd. Gebeurt dit via sms dan heet dit 'SMiShing'.

Met deze **10 tips van Veiliginternetten.nl** bescherm je je smartphone of tablet zo goed als mogelijk tegen mobiele malware. Houd deze tips en adviezen in je achterhoofd als je een app downloadt, op een link in een e-mail of tekstbericht klikt of een openbaar netwerk gebruikt.

1. Download alleen apps in een officiële app store.
2. Klik niet zomaar op links in e-mails en tekstberichten.
3. Verwijder verdachte e-mails en tekstberichten meteen.
4. Log altijd uit als je op een website een betaling hebt gedaan. Sla ook nooit je gebruikersnaam en wachtwoord op in de mobiele browser.
5. Update je mobiele besturingssysteem en apps zodra er een update beschikbaar is.
6. Schakel wifi en bluetooth uit als je dit niet gebruikt.
7. Stuur niet zomaar persoonsgegevens door als daar in een e-mail of tekstbericht om wordt gevraagd.
8. Jailbreak je mobiele apparaat niet. Je apparaat is dan een stuk minder goed beveiligd.
9. Maak regelmatig een back-up van je bestanden.
10. Installeer een beveiligings-app als je er één kunt vinden die aan jouw eisen voldoet.

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Phishing-campagne effectief door koppeling met awareness

‘Lastig zo’n phishing-mail? Tja, dan zeg ik: heb je de tips gelezen?’

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Wie: Martijn Bouckaert
Wat: Hoofd Security Operations Center (SOC)
Waar: Directie Informatisering & Inkoop (DI&I), ministerie van Veiligheid en Justitie

Phishing-campagne
- Start april 2017
- 53.000 ontvangers
- 3 phishing-mails met als lokkertje een waardebon, LinkedIn-uitnodiging en nog een opvolger
- Gemiddeld 12 procent opent phishing-mail

Het oorspronkelijke idee van een platte phishing-campagne leek Martijn Bouckaert, hoofd Security Operations Center VenJ, weinig effectief. 'Dan weet je hoeveel mensen een nepmail openen. En dan?' Bouckaert koppelde de campagne daarom aan een awareness-campagne waarbij handelingsperspectief wordt gegeven. 'De toon is nu: wat doe je als je de nepmail toch hebt geopend? Met die insteek willen we gedrag gaan veranderen.'

Een nepmail sturen en kijken hoe vaak deze wordt geopend. Dat alleen is niet genoeg?

'Nee, want wat bereik je daar nu mee? Dan weet je hoeveel mensen een nepmail openen. En dan? Je houdt bijvoorbeeld altijd een club met notoire klikkers. Die voed je met nog geen honderd campagnes op. Je wilt alle andere collega's handelingsperspectief bieden als het toch een keer misgaat. Wat doe je als je de nepmail toch hebt geopend? Dat is pas interessant en nuttig!'

Dus nu hangt er naast elke computer een lijst met do's & don'ts voor e-mails?

'Cybersecurity door alleen maar nee te zeggen, is geen security. Een lijst met regels werkt niet. Wat wel werkt, is collega's rechtstreeks aanspreken op hun gedrag en verantwoordelijkheid. Daarnaast moet je elkaar vooral de ruimte geven om te leren van fouten. Ik heb liever dat iemand direct bij mij meldt dat hij een phishing-mail heeft geopend, dan dat twee maanden later aan het licht komt dat we een beveiligingslek hebben. Daarvoor is het wel belangrijk dat er geen afrekencultuur heerst.'

Hoe is de phishing-campagne ontvangen?

'Zoals verwacht stuitte ik na het versturen van de eerste mail op weerstand. Sommige collega's hadden liever van tevoren informatie gehad om op in te spelen. Zo is de servicedesk overspoeld met vragen en kregen directieleden en managers veel vragen van personeel. Ik vind dat niet erg. Ik houd wel van een beetje reuring. Dan komen dingen in beweging. En tja, als je iets echt wilt simuleren, moet er een verrassingseffect zijn. Daar leer je ook het meest van met elkaar.'

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

En wat zeg je dan tegen de collega's die weerstand voelen?

'Heb je de informatie en tips gelezen nadat je de nepmail had geopend? We doen dit niet om te pesten. Het gaat erom dat je de volgende keer een nepmail herkent. Iedereen maakt wel eens een fout. Dat geldt ook voor mij. Ik heb de test van de Consumentenbond laatst gedaan om een nepmail te leren herkennen en maakte ook een fout. Dat geeft niet, als je daar maar van leert.'

Een collega van het Nationaal Cyber Security Centrum heeft een andere informatiebehoefte dan het hoofd van een personeelsafdeling. Het is dus nog even zoeken, maar we gaan de collega's zeker bereiken.

Heb je het idee dat het bewustzijn rond cybersecurity toeneemt?

'Ja, er is meer bewustzijn, maar we gebruiken met z'n allen ook meer tools die risico's met zich meebrengen, zoals Dropbox en OneDrive. We moeten dus gezamenlijk alert blijven en de risico's beperken.'

Welke risico's loopt het ministerie van Veiligheid en Justitie?

'Die risico's zijn niet anders dan bij elk ander ministerie of andere overheidsorganisatie. Er is het risico van dataverlies en compromitteren van data. De reputatieschade en politieke schade kan groot zijn. En de grootste nachtmerrie is dat primaire processen worden verstoord. Dat de overheid basale taken als het uitgeven van een paspoort of verblijfsvergunning, het innen van belastingen of de normale rechtsgang niet meer kan uitvoeren.'

Kijk je tevreden terug op de phishing-campagne?

'Absoluut. Ik ben vooral blij met de overwegend positieve reacties van collega's. Ik hoor dat vooral dat de toon van de campagne; opbouwend en niet afstraffend, en het element van awareness gewaardeerd wordt en goed ontvangen is. Daar ben ik heel blij mee omdat dat de effectiviteit van de campagne volgens mij echt heeft vergroot.'

Komt er een vervolg op deze campagne?

'In 2018 wil ik de phishing-campagne herhalen waarbij dan ook de 60.000 collega's van de politie worden meegenomen. Ik wil ook een aparte pagina op het Rijksportaal hebben waar we elke week tips rond een onderwerp kunnen geven. Daarnaast zit ik te denken hoe we op een andere manier handelingsperspectief kunnen bieden. Door een usb-sticks neer te leggen bijvoorbeeld en te kijken hoe mensen daarmee omgaan. Maar dat is lastig voor 53.000 mensen. De omvang van de overheid beperkt soms de mogelijkheden om collega's te bereiken. Daarnaast is het cybersecurity maatwerk.
Dat geldt ook voor het vergroten van het bewustzijn. Een beleidsmedewerker op de Turfmarkt gebruikt de techniek op een andere manier dan een cipier in een justitiële inrichting. Ook wat betreft kennisniveau moet je eigenlijk maatwerk leveren. Een collega van het Nationaal Cyber Security Centrum heeft een andere informatiebehoefte dan het hoofd van een personeelsafdeling. Het is dus nog even zoeken, maar we gaan de collega's zeker bereiken. Tot aan het bureaublad en het schermpje van de smartphone!'

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Zo herken je een phishing-mail

Met deze **6 tips van Veiliginternetten.nl** herken je een phishing-mail voortaan meteen. Zo voorkom je dat je slachtoffer van phishing wordt!

1. Afzender

Controleer het adres van de afzender. De naam van de afzender mag dan precies hetzelfde zijn als die van je bank of webwinkel, maar vaak is het gebruikte e-mailadres een afgeleide versie van een echte bedrijfsnaam of de naam van een instantie. Is het adres onduidelijk en anders dan eerdere mails die je hebt ontvangen? Dan heb je waarschijnlijk met phishing te maken.

2. Aanhef

Word je met hele algemene termen, zoals 'Geachte heer/mevrouw' of 'Beste klant', aangesproken, let dan op. Bedrijven en instanties waar je klant bent, gebruiken meestal in ieder geval je achternaam in een e-mail en weten of je een man of een vrouw bent.

3. Vragen naar persoonsgegevens

In veel nepmails staat het verzoek om je persoonsgegevens 'te controleren', 'bij te werken' of 'aan te vullen'. Je moet dan op een link klikken. Doe dit nooit. Je bank, verzekeringsmaatschappij en overheidsinstanties vragen nooit op deze manier naar persoonsgegevens. Bel het bedrijf of de instantie liever eerst op om te controleren of ze de e-mail wel zelf hebben verstuurd. Gebruik nooit de contactgegevens in de e-mail, maar zoek deze zelf op.

4. Taalgebruik en vormgeving

De huidige generatie nepmails staat allang niet meer altijd bol van de taal- en spelfouten. Ook de gebruikte logo's en foto's worden steeds professioneler. Lees en bekijk de e-mail goed om te zien of je toch geen onregelmatigheden tegenkomt, zoals afwijkende logo's of het verzoek om een rekening met bitcoins te betalen. Je kunt ook een eerdere mail van een bedrijf of instantie ernaast leggen ter vergelijking.

5. Links

Links in nepmails kunnen ervoor zorgen dat er schadelijke software op je computer wordt geïnstalleerd of dat je naar een valse website wordt geleid. Klik dus nooit zomaar op de links in een e-mail die je niet vertrouwt. Controleer het adres van de link door - zonder erop te klikken - de cursor van je muis op de link te zetten en te kijken welk adres er verschijnt.

6. Bijlage

Een bijlage in een nepmail kan ervoor zorgen dat er schadelijke software op je computer wordt geïnstalleerd. Open dus nooit zomaar een bijlage van een e-mail die je niet vertrouwt. Een zip-bestand is altijd verdacht: facturen en aanmaningen worden nooit op deze manier verstuurd. Bel bij twijfel het bedrijf of de instantie op om te controleren of ze de e-mail met bijlage wel zelf hebben verstuurd. Gebruik nooit de contactgegevens in de e-mail, maar zoek deze zelf op.

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Phishing-campagne ministerie Binnenlandse Zaken en Koninkrijksrelaties afgerond

‘Cybercriminelen worden steeds slimmer; vergroten bewustzijn rond cybersecurity bij medewerkers van belang’

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Wie: Annet van Veen
Wat: Adviseur
Waar: CIO-staf, ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)

Phishing-campagne
- Start april 2017
- 11.500 ontvangers
- 3 phishing-mails met als lokkertje een waardebon, LinkedIn-uitnodiging en nog een opvolger
- Gemiddeld 12 procent opent phishing-mail

Twaalf procent van de medewerkers van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft tijdens de phishing-campagne de nepmails geopend. Dat is meer dan gemiddeld aangezien bekend is dat tien procent van de medewerkers overal op klikt. Bij het percentage van twaalf procent moet wel de kanttekening geplaatst worden dat sommige medewerkers waarschijnlijk wisten dat de nepmails onderdeel van de campagne waren, maar dat zij doorklikten omdat ze de info en tips bij elke nepmail wilden lezen.

'Het reële percentage weten we dus niet', zegt Annet van Veen, adviseur CIO-staf van het ministerie. 'Maar wat het percentage ook is, we moeten het zo laag als mogelijk zien te krijgen. En dat begint bij het vergroten van bewustzijn. Want mensen zijn en blijven de zwakste schakel als het om cybersecurity gaat.'

Waarom ben je aangehaakt bij de campagne van het ministerie van Veiligheid en Justitie?

'Omdat ik hetzelfde doel nastreef als de collega's bij VenJ die deze campagne hebben opgezet, namelijk; het vergroten van het bewustzijn van je collega's rond cybersecurity. En aangezien ik het onzin vind om het wiel opnieuw uit te vinden als je samen kunt optrekken, haak ik dus graag aan.'

De campagne is inmiddels afgerond. Ben je tevreden met de resultaten?

'Ja, om meerdere redenen. Ten eerste hebben we 11.500 collega's bereikt met drie phishing-mails, waarmee we het onderwerp meerdere keren onder de aandacht hebben gebracht. Ten tweede, en daar was de campagne niet voor bedoeld, ben ik blij met de 'bijvangst'. Na het versturen van de eerste nepmail heeft een collega bij de ICT-dienstverlener de proxyserver uitgezet, zonder interne afstemming binnen zijn organisatie (de proxyserver = de server die zich bevindt tussen de computer van de gebruiker en de computer waarop de door de gebruiker gewenste informatie staat). In een 'echte' situatie een alerte actie, maar bij de simulatie ongewenst omdat de phishing-mail nu niet verzonden werd. Met het oog op een 'echt' incident, een mooie aanleiding om rollen, processen en de wijze van communiceren opnieuw te bekijken.'

En moest die collega bij de ICT-dienstverlener nog op het matje komen?

'Nee, absoluut niet! Dat wil ik nog even benadrukken: deze campagne is gericht op het vergroten van kennis over cybersecurity; je zou het kunnen zien als een BZK-brede e-learning. Leren en ontwikkelen lukt het best in een veilige omgeving waar fouten bespreekbaar zijn. Het klikken op een phishing-mail, vooral omdat ze steeds beter worden, is

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

niet iets waarvoor je je hoeft te schamen. Wel is het handig om te weten hoe je de phishing-mail had kunnen herkennen zodat je het klikken op een phishing-mail in de toekomst kunt voorkomen. Om die reden is de campagne geanonimiseerd. Zichtbaar wordt het aantal maal dat op een link is geklikt, maar niet door wie.'

Is phishing niet eenvoudig te voorkomen door te investeren in ICT? Betere virusscanners en firewalls bijvoorbeeld.

'Was het maar zo eenvoudig. Techniek ondervangt niet alles. Mensen zijn de zwakke schakel als het om cybersecurity gaat. Laatst zag ik cijfers waaruit bleek dat techniek 34 procent van de bedreigingen, zoals phishing-mails en malware, ondervangt. Dan houd je dus 66 procent van de bedreigingen over die door mensen gestopt moeten worden. Gebruikers worden slachtoffer van cybercriminelen doordat zij zich onvoldoende bewust zijn van de risico's van hun acties of door verkeerd handelen. Vandaar dat BZK haar medewerkers het hele jaar informeert over hoe zij bewust en veilig om kunnen gaan met informatie (online en offline).'

Wil je doorgaan met het vergroten van het bewustzijn rond cybersecurity?

'Zeker. Continuïteit rond het onderwerp is belangrijk zodat medewerkers de ontwikkeling van onbewust onveilig (= ik ben me er niet van bewust dat ik onveilig werk) naar onbewust veilig (= ik ga 'automatisch' op een veilige manier met informatie om en hoef daar niet meer over na te denken) doorlopen. In het begin voelt dit wellicht als een 'plus' op je werkzaamheden. Je moet bewust stilstaan en nadenken over je handelen, bijvoorbeeld het vergrendelen van je beeldscherm. Maar dit went snel, zeg ik uit ervaring.'

Dat wil ik nog even benadrukken: deze campagne is gericht op het vergroten van kennis over cybersecurity, je zou het kunnen zien als een BZK-brede e-learning

Welke activiteiten kunnen collega's nog verwachten?

'Tijdens Alert Online organiseren we een bijeenkomst waarbij iemand van het Centraal Meldpunt Identiteitsfraude- en fouten (CMI), een gemeenteambtenaar, een politieagent en een slachtoffer vertellen over identiteitsfraude. Ook organiseren we in het kader van Alert Online een serious game waarbij getoond wordt hoe hackers werken en hoe jouw brein daarop reageert. Na Alert Online wil ik doorpakken met maandelijkse storytelling waarbij verschillende onderwerpen aan bod komen, zoals wachtwoordbeheer en wifi bijvoorbeeld.'

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

PHISHING: laat je niet vangen!

De phishing-campagne van Veiliginternetten.nl is bedoeld om je te helpen om pogingen tot phishing in de toekomst te herkennen, je te vertellen welke stappen je moet nemen als je slachtoffer van phishing bent én je te laten zien hoe je je apparaten zo goed als mogelijk kunt beschermen tegen cybercriminaliteit.

Voor meer informatie over phishing, zoals de tips om nepmail te herkennen, ga je naar de campagnepagina van Veiliginternetten.nl: veiliginternetten.nl/phishing/.

Phishing-quiz
Wat weet jij eigenlijk over phishing?
Test je kennis met de phishing-quiz: veiliginternetten.nl/quiz-campagne-phishing-2017/.

Over Veiliginternetten.nl
Veiliginternetten.nl is een website, waar mensen tips, tricks en praktische stap-voor-stap uitleg kunnen vinden over wat zij moeten doen en laten om veilig te internetten. Ze vinden er tips hoe ze veilig omgaan met hun online privacy, hoe ze veilig gebruik maken van wifi, wat ze kunnen doen en laten op sociale media, en ze vinden er uitleg over hoe zij kinderen helpen veilig online te zijn. Deze site is bedoeld voor iedereen met vragen over veilig gebruik van internet.

Leestips online veiligheid

Wil je meer lezen over online veiligheid? De actualiteiten volgen of je kennis vergroten? We hebben een aantal leestips voor je op een rij gezet. Hieronder een overzicht van websites, boeken en media die je kunnen helpen je kennis en vaardigheden te vergroten om veilig online te zijn. Of die gewoon leuk zijn om te lezen en te volgen!

Ben jij gehackt?

Controleer op de website van de politie of de gegevens van jouw (persoonlijke) e-mailaccount zijn gestolen.

Websites:

Rijksoverheid.nl
Lees hoe je identeitsfraude kunt voorkomen. Bijvoorbeeld door de KopieID-app te gebruiken.

Rijksoverheid.nl
Slachtoffer van identiteitsfraude? Het Centraal Meldpunt Identiteitsfraude en -fouten (CMI) ondersteunt en adviseert slachtoffers van identiteitsfraude.

Veiliginternetten.nl
Veilig internetten is een website waar mensen tips, tricks en praktische stap-voor-stap uitleg kunnen vinden over wat zij kunnen doen en laten om veilig te internetten.

Fraudehelpdesk.nl
De Fraudehelpdesk is er voor al jouw vragen en meldingen over fraude.

Meldknop.nl
Via Meldknop.nl krijgen jongeren tussen de 11 en 16 jaar informatie en advies om internetproblemen op te lossen.

Consumentenbond.nl
De Consumentenbond is een vereniging in Nederland die opkomt voor de belangen van consumenten.

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Nomoreransom.org
Slachtoffer van ransomware? No More Ransom helpt bij het herstellen van versleutelde bestanden zonder betaling aan criminelen.

Centrum Informatiebeveiliging en Privacybescherming
(www.cip-overheid.nl)
CIP is het expertisecentrum voor informatie-beveiliging en privacybescherming. Van, voor en door overheidsorganisaties.

Op de sites van tv-programma's Opgelicht?! en Kassa vind je nieuwtjes over malware en nepmails die in omloop zijn.

Boeken:

Je hebt wél iets te verbergen,
Maurits Martijn en Dimitri Tokmetzis

Helpende Hackers,
Chris van 't Hof

Bescherming tegen cybercrime,
Brenno de Winter

Komt een vrouw bij de hacker,
Maria Genova

Vlog
Vlog van Isabel Provoost over het tegen gaan van Phising

Media:

Tektok.nl
Tek Tok Late Night is een praatprogramma over informatietechnologie op verschillende locaties in Nederland en via een YouTube-kanaal.

GDI.Foundation
GDI.Foundation is een non-profitorganisatie die zoekt naar kwetsbaarheden in IT-systemen. Deze melden zij bij organisaties via responsible disclosure.

Bits of Freedom
Bits of Freedom verdedigt burgerrechten op het internet en zet zich in voor een open internet dat toegankelijk is voor iedereen, waar privé-communicatie privé blijft en waar iedereen informatie met elkaar kan blijven delen.

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Alert Online

Wat is er allemaal te doen van 2 – 13 oktober 2017?

Het kan iedereen overkomen: je klikt op een link in een e-mail of downloadt per ongeluk een bestand met een virus. Cybercriminelen worden steeds slimmer en gebruiken trucjes om jouw gegevens in handen te krijgen.

Cybersecurity: techniek, mens en organisatie

Alert Online maakt zich hard voor bewustwording over cybersecurity; veilig omgaan met informatie ter voorkoming van uitlekken, kwijtraken of diefstal van informatie bij burgers, bedrijfsleven en overheden. Vooral omdat in *ruim 60%* van de gevallen *de mens de zwakste schakel* in het beveiligingsproces is. Naast het verstrekken van informatie om jouw kennis over cybersecurity te vergroten, gaat het bij Alert Online vooral om het besef dat **je zélf** van alles kunt doen om veilig en bewust te werken met informatie.

Initiatief

Alert Online is een jaarlijks initiatief van de overheid, het bedrijfsleven en de wetenschap met als doel Nederland online veiliger te maken. Samen zetten we ons in om de bewustwording over hoe je online en offline veilig kunt omgaan met informatie te vergroten. De technologische ontwikkelingen gaan snel, bieden kansen maar brengen ook risico's met zich mee. Hoe goed ben jij op de hoogte van de laatste ontwikkelingen, bijvoorbeeld ransomware? En wat betekent flexibel werken en het delen van een werkplek voor de wijze waarop je met informatie omgaat?

Hoe veilig en bewust werk jij met informatie? Doe mee met de Alert Online-weken en kies uit het aanbod van activiteiten die je helpen om bij cybersecurity stil te staan. In deze nieuwsbrief vind je een overzicht van wat er allemaal te doen is binnen BZK en VenJ. Want deze campagne doen we in gezamenlijkheid.

Alert Online Agenda

Dinsdag 3 oktober

Locatie Turfmarkt 147 | 11.30-14.30 uur | Bedrijfsrestaurant, 3e etage | Scheg

What the #hack?! – lunch workshop

Kruip achter de pc en ga zelf aan de slag als hacker! Ervaar tijdens de workshop hoe een hacker zwakke plekken in de beveiliging zoekt. Ontdek wat je kunt doen om de hacker een stap voor te zijn. **Aanmelden**

Woensdag 4 oktober

Locatie Turfmarkt 147 | 8.30-10.00 | Auditorium

De menselijke factor van online dreiging - ontbijtlezing

Te vaak wordt voorkeur gegeven aan technologische maatregelen als het gaat om weerbaarheid tegen digitale dreiging. De menselijke factor blijft daarin onderbelicht. Elsine van Os gaat in haar presentatie in op de integratie van psychologie en technologie bij insider threat-management.
(ontbijt van 8.30 tot 9.00 uur, aansluitend tot 10.00 uur lezing). **Aanmelden**

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Woensdag 4 oktober
Rijksportaal | achter de eigen pc
Test je kennis met allerlei **online quizzen**: een CyberskillsTest, een Phishing-quiz en de e-learningmodules iBewustzijn.

Donderdag 5 oktober
Locatie Turfmarkt 147 | 9.00-11.00 | Amaliazaal
Identiteit gestolen, wat dan? – ontbijtlezing
Beveiligen van gegevens, je hoort het constant om je heen. Hoe bescherm jij jezelf tegen identiteitsfraude? En wat te doen als je identiteit is gestolen? Wat kan er precies gebeuren als (jouw) gegevens in verkeerde handen vallen? Dat hoor je tijdens deze sessie van een spreker van het Centrum Meldpunt Identiteitsfraude. Zij neemt je mee in de gevolgen van identiteitsfraude, zodat je weet wanneer je hiermee te maken hebt en wat je kunt doen om je hiertegen te beschermen. Verder krijg je via een spreker van de politie inzicht in de manier waarop zij omgaan met het vaststellen van iemands identiteit en waar ze tegenaan lopen. (ontbijt van 9.00 tot 9.30 uur, aansluitend tot 11.00 uur lezing). **Aanmelden**

Vrijdag 6 oktober
Rijksportaal | achter de eigen pc
Interview met Terry Hasselo (BVA) en Hans de Vries (NCTV).
"De digitale weerbaarheid in Nederland blijft achter bij de groei van dreigingen. Overheid, bedrijfsleven en burgers nemen veel stappen om de digitale weerbaarheid te vergroten, maar dit gaat niet snel genoeg. Dat blijkt uit het Cybersecuritybeeld Nederland 2017 (CSBN 2017) dat demissionair staatssecretaris Dijkhoff naar de Tweede Kamer heeft gestuurd." https://www.ncsc.nl/actueel/Cybersecurity-beeld+Nederland/cybersecuritybeeld-nederland-2017.html

Maandag 9 oktober
Locatie Turfmarkt 147 | 9.00-11.00 | Auditorium
De zwakste schakel: de psychologie van informatiebeveiliging - ontbijtlezing
Mediapsycholoog Mischa Coster gaat dieper in op de menselijke kant van cybersecurity. Welke invloed heeft jouw brein op je handelen? Hoe benutten kwaadwillenden dit om aan jouw gevoelige informatie te komen? (ontbijt van 9.00 tot 9.30 uur, aansluitend tot 11.00 uur lezing) **Aanmelden**

Dinsdag 10 oktober
Locatie Turfmarkt 147 | 9.00-11.30 uur | Workshopruimte Z02-423
Serious game 'Crisis' – rollenspel met als doel het verwerven van inzicht. Een cybercrimineel heeft jouw organisatie gehackt. Hoe reageer je hierop, hoe handel je en hoe communiceer je naar partijen? Doe mee en beleef het mee! **Aanmelden**

Woensdag 11 oktober
Rijksportaal | achter de eigen pc, inloggen via de Belastingdienstacademie
*Speel de online-game 'Lek!' via de **Belastingdienst-academie**.*

Donderdag 12 oktober
Locatie Turfmarkt 147 | inloop vanaf 15.30 uur | Auditorium
VenJ Café meets Cybersecurity: techniek, mens en organisatie
Zijn wij ons met elkaar wel voldoende bewust van ons eigen veiligheidshandelen? En hoe zorgen we ervoor dat we bewust blijven als het gaat om informatieveiligheid?
Wat is phishing en wat je moet doen als je ermee geconfronteerd wordt? Over dit soort zaken kun je meer horen in het VenJ IV Café van 12 oktober. De mogelijke dreiging vanuit cybercrime is een zaak die iedereen binnen de veiligheidsketen raakt. Nut en noodzaak van verbinding en samenwerking worden breed gedragen, maar de praktijk is weerbarstig. Zeker op het snijvlak van veiligheid en transparantie. In het VenJ IV Café wordt die samenhang zichtbaar door de lezingen van een aantal sprekers vanuit onder meer het Nationaal Cyber Security Centrum, het OM en de Rechtspraak. Het concept: 4 sprekers geven een presentatie op basis van Pecha Kucha (6 minuten en 40 seconden per spreker). Aansluitend gelegenheid voor vragen/discussie, en een afsluitende netwerkborrel. Luister, beleef en huiver! Meld je aan via de link. **Aanmelden**

Maandag 16 oktober
Rijksportaal | achter de eigen pc
Terugblik op twee weken Alert Online.

Meer weten over cybersecurity?
Website **Alert Online:** doe de CyberskillsTest en laat je inspireren door handige tips.
Website **Veilig Internetten:** praktische informatie en uitleg om veilig te internetten.

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

COLUMN

Don’t feed the phish

Door: Mischa Rick van Geelen - NFIR

Phishing is wereldwijd een steeds lucratievere business, ook in Nederland zie ik dat er een toename in verstuurde mails is met het doel om geld te stelen, informatie te verzamelen of organisaties aan te vallen. Ik zie dit in de komende jaren alleen nog maar vergroten, omdat organisaties in Nederland nog niet volledig voorbereid zijn op deze aanvallen.

Spear phishing
Vooral spear phishing blijkt een effectief middel te zijn, omdat dit type e-mails het doel heeft om zo persoonlijk mogelijk te zijn waardoor de geloofwaardigheid van de e-mails omhoog gaat. Juist door het toepassen van dit soort technieken worden nog steeds op dagelijkse basis veel organisatie gehackt en informatie gestolen.
Het is dan ook belangrijk dat organisaties in Nederland een bewustzijn krijgen over hoe ze een phishing e-mail kunnen herkennen en kunnen voorkomen dat de organisatie daarbij gecompromitteerd wordt.

Het is belangrijk dat organisaties in Nederland een bewustzijn krijgen over hoe ze een phishing e-mail kunnen herkennen en kunnen voorkomen dat de organisatie daarbij gecompromitteerd wordt

CEO-fraude
Iets wat ik ook steeds meer zie is CEO-fraude via e-mail, waarbij er door een aanvaller van buitenaf een e-mail verstuurd wordt naar de financiële afdeling van een organisatie die lijkt te komen van de bestuurder of CEO. In deze e-mail wordt veelal het verzoek gedaan om een spoedbetaling uit te voeren, omdat deze bijvoorbeeld van belang is voor de organisatie. In werkelijkheid vraagt een aanvaller om geld over te maken naar een onbekend rekeningnummer, met alle gevolgen van dien.

Don’t feed the phish
Een belangrijk deel van het verminderen van de problemen en gevolgen rond om phishing is het bewust worden van het feit dat alles wat in de mailbox terecht komt in principe schadelijk kan zijn. Ook als dit van een collega of vertrouwd contactpersoon komt.
Veelal wordt dit bewustzijn gecreëerd door awareness sessies, waarbij de deelnemers via interactieve sessies kunnen meemaken wat de gevolgen van een phishing e-mail zijn en hoe je kan herkennen wat een phishing e-mail is.
Wat ik veel organisaties dan ook adviseer is om jaarlijks awareness sessies te organiseren om het bewustzijn onder de medewerkers hoog te houden, en werknemers het gevoel te geven dat ze in staat zijn om zich te verdedigen tegen dit soort aanvallen.

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Online veiligheid en bewustzijn kennen geen eindstation meer

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Wie: Ronald Barendse
Wat: Plaatsvervangend secretaris-generaal
Waar: Ministerie van Veiligheid en Justitie (VenJ)

Wie: Emine Özyenici
Wat: Directeur informatievoorziening
Waar: Directie informatisering en inkoop (DI&I), ministerie van Veiligheid en Justitie (VenJ)

Wie kwam er met het idee voor de phishing-campagne? En waarom is het vergroten van bewustzijn over online veiligheid zo belangrijk? Tijdens een dubbelinterview geven Ronald Barendse, plaatsvervangend secretaris-generaal, en Emine Özyenici, directeur informatievoorziening, antwoord op deze vragen. Én op de vraag of zij privé ook actief bezig zijn met online veiligheid.

Wie kwam er met het idee voor de phishing-campagne?

Ronald: 'Het idee ontstond tijdens een overleg met oud-minister Ard van der Steur en Dick Schoof, de Nationaal Coördinator Terrorismebestrijding en Veiligheid. Hoe is het eigenlijk met ons eigen niveau van bewustzijn? Hebben wij ons eigen huis op orde? Dat waren de vragen die wij onszelf stelden.'
Emine: 'En tijdens dat overleg werd het idee van een phishing-campagne ook meteen heel concreet. Iedereen vond het een goed middel om zoveel mogelijk collega's te bereiken. Er is naderhand wel nog besloten om de campagne niet alleen te beperken tot het versturen van nepmails, maar om ook het onderdeel bewustwording eraan toe te voegen. Bewustwording door middel van info en tips op de landingspagina van de nepmails, maar ook via dit magazine bijvoorbeeld.'

Waarom is zo'n campagne belangrijk voor VenJ?

Emine: 'Het is ook belangrijk omdat online veiligheid en bewustzijn geen eindstation meer kennen. Daarvoor gaan de technologische ontwikkelingen en de komst van nieuwe bedreigingen te snel. We moeten er niet alleen als ministerie, maar ook als samenleving, voor zorgen dat we niet achteropraken. Doordat we meer technologie in ons werk en persoonlijke leven toelaten, nemen de risico's ook toe.'
Ronald: 'Binnen ons ministerie bevindt zich veel gevoelige informatie. Wij zijn derhalve misschien een interessant doelwit. Door iedereen meer bewust te maken van de gevaren én te stimuleren om online veiligheid serieus te nemen, hoop ik dat onze weerbaarheid toeneemt. Daarom is de insteek van de campagne ook *awareness*, bewustzijn vergroten, en de gekozen vorm phishing.'

Wat doet VenJ allemaal al om de online veiligheid te waarborgen?

Ronald: 'We hebben de handen op elkaar gekregen voor de oprichting van een collectief departementaal SOC VenJ, een Security Operations Center. Dat is een mooie en noodzakelijke stap die we met elkaar zetten. Het SOC zal in de toekomst het netwerk 24 uur per dag monitoren op hackers, malware en virussen.'
Emine: 'Voor medewerkers zijn er natuurlijk al de richtlijnen en gedragscodes waarin staat hoe je om moet gaan met informatie en de apparaten die je gebruikt. Daarnaast staan de collega's van de SSC-ICT servicebalies altijd klaar voor hulp en advies. Bijvoorbeeld in het geval van een defect apparaat, het resetten van wachtwoorden en andere ICT-gerelateerde vragen.'

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

We signaleren dat het onderwerp cybersecurity ontzettend leeft en dat iedereen gemotiveerd is om het onderwerp op de agenda te houden.

Hoe waren de reacties op de campagne?

Emine: 'Van hoog tot laag heeft de campagne impact gehad. Dat is geweldig. Het onderwerp online veiligheid is echt op de kaart gezet. Mochten we ooit nog een phishing-mail gaan versturen, zou ik wel iets meer afstemming willen wat betreft de inhoud van de nepmail. Zo kreeg ik op de eerste nepmail, waar een cadeaubon het lokkertje was, stevige reacties van beleidsmedewerkers. 'Wie bedenkt dit?! Cadeaubonnen weggeven...', was de vraag.'
Ronald: 'Goed. We signaleren dat het onderwerp cybersecurity ontzettend leeft en dat iedereen gemotiveerd is om het onderwerp op de agenda te houden. Het was belangrijk om na elke verzonden nepmail een update te krijgen over hoeveel mensen de mail hebben geopend. Daar zijn mensen benieuwd naar. Dat moet je tussentijds kunnen communiceren.'

Hoe zorg je ervoor dat het bewustzijn rond phishing, en andere vormen van cyber-criminaliteit, niet wegzakt na afloop van de campagne?

Emine: 'Ik vind dat ik als leidinggevende een taak heb om collega's actief te wijzen op updates, bijvoorbeeld als er een dreiging zoals ransomware is. Even prikkelen; iedereen erop attenderen. Ik zie het echt als een onderdeel van mijn pakket aan managementtakken. Zoals het terugdringen van ziekteverzuim dat bijvoorbeeld ook is.'

Kennen jullie mensen die slachtoffer van cybercriminaliteit zijn?

Ronald: 'Nee, ik ken niemand die online slachtoffer is geworden.'
Emine: 'Ik ook niet. Wat wel een keer is gebeurd, over bewustzijn gesproken, is dat ik door een collega-directeur werd gebeld. Hij zat in de trein en twijfelde over een e-mail. 'Emine, ik heb een mailtje en ik durf hem niet te openen', zei hij. 'Jij weet van de phishing-campagne, dus ik bel jou maar.' Dat vond ik dus echt heel goed. Hij was bewust en durfde te vragen of dit mailtje veilig was. De e-mail bleek uiteindelijk veilig.'

Zijn jullie privé ook actief bezig met online veiligheid?

Ronald: 'Mijn basisbeveiliging is thuis op orde. Updates worden direct geïnstalleerd en ik gebruik een betaalde virusscanner. Daarnaast hebben we thuis via de internetprovider een extra pakket dat spam en andere rommel filtert. Maar ook ik moet soms weer even worden wakker geschud en heb dan een zetje nodig om instellingen weer eens goed na te lopen.'
Emine: 'Ik ben getrouwd met een ICT-consultant dus de beveiliging privé is op orde. Het is bij ons altijd onderwerp van gesprek. Behalve dat alles goed staat ingesteld, heb ik ook mijn gedrag aangepast. Waar ik bij vroegere werkgevers nog weleens e-mails naar mijzelf mailde om thuis door te kunnen werken, doe ik dat sinds ik bij VenJ werk niet meer. Ook zet ik mijn desktop standaard uit als mijn werkplek verlaat.'

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Veiliginternetten.nl biedt info en praktische tips om de online veiligheid te vergroten

‘Je online veiligheid neemt fors toe als je phishing-mails kunt herkennen’

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Wie: Stijn Jaspers
Wat: Webredacteur
Waar: Veiliginternetten.nl, ECP I Platform voor de InformatieSamenleving

Veiliginternetten.nl
Veiliginternetten.nl is een website waar consumenten en zakelijke gebruikers tips, tricks en praktische stap voor stap uitleg kunnen vinden over wat zij kunnen doen en laten om veilig te internetten. Veiliginternetten.nl is een gezamenlijk initiatief van het ministerie van Economische Zaken, het ministerie van Veiligheid en Justitie / Nationaal Cybersecurity Centrum, ECP | Platform voor de InformatieSamenleving en het bedrijfsleven.

Volgens Stijn Jaspers, webredacteur van Veiliginternetten.nl, is het vergroten van je online veiligheid helemaal niet zo moeilijk. 'Wie zich consequent houdt aan een aantal basisregels loopt veel minder risico om slachtoffer van phishing te worden of van een andere vorm van cybercrime.'

Waarom trappen mensen eigenlijk nog in phishing-mails? Die staan toch bol van de spelfouten en vage logo's waardoor iedereen ze inmiddels wel herkent?

'Dat is helaas niet zo. Phishing-mails zijn steeds vaker nauwelijks van een echte e-mail te onderscheiden. Zelfs de websites achter de links in een phishing-mail worden exact gekopieerd. Op deze websites worden mensen verleid om zakelijke of persoonlijke info in te vullen. Het is dus niet raar dat internetgebruikers erin trappen.'

Maar wat kun je dan doen om jezelf te beschermen?

'Wie zich consequent houdt aan een aantal basisregels loopt veel minder risico om slachtoffer van phishing te worden of van een andere vorm van cybercrime. Belangrijk is dat je altijd scherp blijft bij het openen van een e-mail. Ziet het afzendadres er legitiem uit? Nee, gooi de mail weg. Word je gevraagd om per ommegaande een betaling te doen of iets in te vullen? Pas op! Bevat de e-mail een bijlage met een .zip- of .exe-bestand? Open deze bijlage niet!'

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Dat zijn rechttoe-rechtaan tips. ‘Is het echt zo simpel?‘

Eigenlijk wel ja. Het vergroten van je online veiligheid is helemaal niet zo moeilijk. Natuurlijk ben je als organisatie, bedrijf of consument ook afhankelijk van de techniek. Maar een firewall en virusscanner vangen niet alles af. De mens is en blijft de zwakste schakel. Gelukkig kun je heel veel zelf doen om je online veiligheid te vergroten. De praktische stappenplannen op Veiliginternetten.nl helpen internetgebruikers daarbij.’

Als we ons allemaal realiseren wat de risico’s zijn en daar consequent naar handelen, komen we echt een heel eind om phishing, en andere cybercrime, terug te dringen.

Is phishing een van de meest populaire vormen van cybercrime?

‘Ja, want het maakt gebruik van de zojuist genoemde zwakste schakel: de mens. Het is best moeilijk voor een cybercrimineel om gericht in systemen in te breken. Daar is flink wat technische kennis voor nodig. Door met één druk op de knop naar duizenden mensen een phishing-mail te sturen, komt hij veel sneller binnen. Phishing maakt cybercriminaliteit daardoor helaas ook een stuk laagdrempeliger. Je hoeft echt geen programmeur meer te zijn om cybercrime te plegen. De tools en programma’s zijn online verkrijgbaar, waardoor je relatief makkelijk je eigen phishing-campagne start.’

Het gevecht tegen phishing, is dat eigenlijk wel te winnen?

‘Nooit helemaal natuurlijk. Net als ‘gewone’ misdaad zal ook cybercrime blijven bestaan. Daarvoor is het gewoon te lucratief. Er zullen ook altijd mensen blijven die zich online risicovol gedragen. Maar dat betekent niet dat niet iedereen die online is het gevecht moet aangaan. Je moet er in elk geval voor zorgen dat je jezelf zo goed als mogelijk kunt verdedigen. Dat begint bij bewustwording, gevolgd door gedragsverandering. Als we ons allemaal realiseren wat de risico’s zijn en daar consequent naar handelen, komen we echt een heel eind om phishing, en andere cybercrime, terug te dringen. Volgens mij is bij het Ministerie van Veiligheid en Justitie, en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties die bewustwording nu echt ingezet dankzij de phishing-campagne. Ik nodig nu dan ook iedereen uit om Veiliginternetten.nl te bezoeken voor concreet handelingsperspectief. Want wie zich bewust is van de dreigingen, vindt op onze website veel info en praktische tips om de cybersecurity direct te vergroten.’

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Imago en huisstijl CJIB populair onder cybercriminelen

CJIB mailt nooit een boete of aanmaning

Burgers oplichten door hen via e-mail een boete uit naam van het Centraal Justitieel Incassobureau (CJIB) te sturen. Deze vorm van oplichting is een van de meest populaire onder cybercriminelen. Er zijn inmiddels tientallen varianten van CJIB-spookfacturen bekend. Hoeveel burgers zo'n e-mail hebben ontvangen, is niet precies bekend, maar het zullen er héél veel zijn.

Hoe kun je als uitvoeringsorganisatie nu voorkomen dat imago en huisstijl misbruikt worden door cybercriminelen? 'Je kunt als uitvoeringsorganisatie niet voorkomen dat je imago en huisstijl misbruikt worden. Wat je wel kunt doen, is stevig inzetten op het waarschuwen en voorlichten van het grote publiek', zegt Anne Tuinstra, adviseur communicatie. 'Het CJIB mailt nooit een boete of aanmaning. Heb je dus een mail ontvangen waarin staat dat je een boete moet betalen? Dan is dit altijd een nepmail van oplichters, die zo aan jouw geld proberen te komen!'. Het CJIB is overigens niet de enige uitvoeringsinstantie waarvan imago en huisstijl misbruikt worden. Phishing door cybercriminelen vindt ook plaats door het versturen van

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

nepmails uit naam van onder andere de belastingdienst, het UWV (Uitvoeringsinstituut Werknemersverzekeringen), de SVB (Sociale Verzekeringsbank) en DUO (Dienst Uitvoering Onderwijs). Vooral uitvoeringsinstanties hebben last van deze vorm van cybercriminaliteit. Wij proberen daarom binnen de Manifestgroep dit onderwerp op de agenda te krijgen', zegt Anne. De Manifestgroep is een netwerk van 16 uitvoeringsorganisaties van het Rijk en trekt gezamenlijk op om de dienstverlening aan burgers en bedrijven te verbeteren.

'Nogmaals, we kunnen misbruik niet voorkomen, maar waren ons bij de introductie van de nieuwe beschikking heel erg bewust van het feit dat burgers deze als nep zouden kunnen beschouwen, omdat ze zoveel spookfacturen, zogenaamd uit naam van het CJIB, ontvangen'

'Aan elke nieuwe mailvariant is het CJIB veel tijd kwijt. Met het beantwoorden van vragen van bezorgde burgers en het communiceren over welke spookfacturen in omloop zijn. Ook doet het CJIB altijd aangifte van misbruik van beeld- en woordmerk. Dat kost ook tijd. We zouden graag binnen de Manifestgroep samen naar manieren zoeken om onszelf en de samenleving tegen cybercriminaliteit te beschermen. Een gezamenlijke bewustzijnscampagne is een van de ideeën', vertelt Anne. Dat deze vorm van cybercriminaliteit invloed heeft op de dienstverlening van het CJIB, werd erg duidelijk tijdens de introductie van de nieuwe verkeersboete, afgelopen zomer. 'Nogmaals, we kunnen misbruik niet voorkomen, maar waren ons bij de introductie van de nieuwe beschikking heel erg bewust van het feit dat burgers deze als nep zouden kunnen beschouwen, omdat ze zoveel spookfacturen, zogenaamd uit naam van het CJIB, ontvangen', volgens Anne. De verkeersboete heeft een nieuw uiterlijk. Zo is het nu in één oogopslag duidelijk wat voor overtreding je waar en wanneer hebt gemaakt.

Ook is sinds 2 maanden de acceptgirokaart verdwenen van de verkeersovertredingen (WAHV). Alle informatie om het bedrag over te maken vind je nu op de vernieuwde boete. **Klik hier** voor de pagina op CJIB.nl met daarop alle informatie over de vernieuwde verkeersboete. Volgens Roel Wubben, integrale beveiligingsfunctionaris, zal de vernieuwing cybercriminelen niet laten stoppen met het sturen van CJIB-spookfacturen. 'Tegengaan van phishing was ook niet het doel van een nieuw uiterlijk. De vernieuwing is bedoeld om moderner en eenduidiger te communiceren. Wat cybercriminelen vervolgens met jouw imago en huisstijl doen, heb je helaas niet in de hand. Dat gebeurt buiten ons bereik om.' Daarmee blijft de belangrijkste tip om jezelf tegen een CJIB-spookfactuur te beschermen: heb je een mail met een boete of aanmaning ontvangen? Gooi deze dan weg. Het CJIB mailt nooit een boete of aanmaning! En als je twijfelt over de verkeersboete die op de deurmat valt, controleer dan in het **Digitaal Loket** van het CJIB of er echt een verkeersboete voor je klaarstaat.

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Dubbelinterview Wendy Sutherland en Hylke Wierda

‘Technologische ontwikkelingen gaan heel snel, verslappen is geen optie’

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

Wie: Wendy Sutherland
Wat: Directeur Concernondersteuning
Waar: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)

Wie: Hylke Wierda
Wat: plv. CIO / plv. directeur CIO & Informatiemanagement
Waar: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)

Grote uitdagingen op het digitale domein in een tijd dat flexibel werken een grote vlucht neemt, zorgen ervoor dat we een groot belang hechten aan de wijze waarop medewerkers met informatie omgaan: het I-bewustzijn. Daarom is BZK voor de derde maal een grote campagne gestart om het I-bewustzijn van de medewerkers te verhogen. Wendy Sutherland, directeur Concernondersteuning en Hylke Wierda, plv. CIO BZK, geven hun visie op de uitdagingen waar BZK voor staat.

Jullie hebben bij BZK al voor de derde keer een grote campagne gevoerd rondom I-bewustzijn. Waarom is dat zo belangrijk voor jullie?

Wendy: 'BZK heeft als departement een belangrijke en bijzondere rol. We zijn onder meer verantwoordelijk voor democratie, het openbaar bestuur en de grondwet. Maar we hebben ook grote 'shared service organisaties' in huis, die diensten leveren aan andere departementen. Als directeur Concernondersteuning vind ik het belangrijk dat we onze medewerkers optimaal ondersteunen bij het uitvoeren van al die taken. Daar hoort ook bij dat medewerkers instrumenten aangereikt worden. Dat varieert van een goede werkplek tot heldere gedragsrichtlijnen.'
Hylke: 'Met een campagne kunnen we het beschikbare instrumentarium ook heel makkelijk onder de aandacht brengen. Het biedt een handvat om het gesprek te voeren over hoe je werkt en wat je met je informatie doet. De phishing-campagne helpt om dat gesprek goed te voeren. En dat gaat wat mij betreft breder dan alleen het beveiligingsvraagstuk. Natuurlijk moeten mensen zich bewust zijn van de risico's, maar het gaat verder. Het heeft wat mij betreft ook te maken met hoe je samen werkt, samen informatie deelt, opslaat en bewaart.'

Flexwerken heeft daar natuurlijk ook een effect op?

Wendy: 'Ja, zeker. Flexibilisering heeft veel positieve effecten, maar het brengt ook vragen met zich mee. Hoe zorg je dat medewerkers elkaar goed kunnen blijven informeren als je elkaar niet voortdurend op de werkplek treft, bijvoorbeeld? Maar niet alleen flexibilisering is van belang. In het rapport 'Maak waar' wordt ook heel duidelijk aangegeven dat digitalisering een hele andere cultuur vraagt van onze organisatie. Digitalisering wordt gezien als belangrijk en urgent, en dat betekent ook dat we als organisatie zelf

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

daar strategisch naar moeten blijven kijken. Digitalisering is immers niet alleen een technisch vraagstuk, maar raakt aan tal van andere zaken op het gebied van bestuur, beleid, communicatie, personeels- en organisatieontwikkeling.'
Hylke: 'We zien dat digitalisering natuurlijk niet bij de randen van de organisatie ophoudt. Inmiddels is ICT onlosmakelijk verbonden met het maken en uitvoeren van beleid. Of het nu is omdat er nagedacht moet worden over onderliggende systemen en applicaties, of de informatiestromen; het heeft allemaal te maken met verdergaande technologische ontwikkelingen en mogelijkheden. Dan is het van belang dat medewerkers daarin ook meegenomen worden; zowel in de mogelijkheden die het biedt, als in de risico's die het met zich meebrengt.'

Wat doen jullie dan concreet om hieraan een bijdrage te leveren?

Wendy: 'Onze medewerkers werken digitaal, delen gegevens en dan is het ook van belang dat zij daar zorgvuldig mee omgaan. We proberen, zeker ook met de flexibilisering, mensen optimaal te ondersteunen, ook als ze thuis of elders buiten kantoor werken. Dus we zorgen voor goede apparatuur en toegang, maar ook voor duidelijke spelregels. Daarnaast hebben we afgelopen jaren geïnvesteerd in onze security governance. Daarmee bedoel ik dus maatregelen die we nemen om de informatiebeveiliging verder te versterken en te bestendigen.'
Hylke: 'De campagne Alert Online zorgt ook voor veel aandacht voor informatieveiligheid. Maar we willen dat natuurlijk bestendigen, dus door het jaar heen bieden we opleidingen en kennissessies aan. Ook attenderen we onze medewerkers erop hoe je in algemene zin met informatie om moet gaan. Over hoe en waar je je informatie hoort op te slaan, de clean desk policy en regels rond gebruik van sociale media. Dat moet allemaal bijdragen aan een veiliger klimaat. We merken ook dat het in een behoefte voorziet. We krijgen veel vragen en ik merk dat medewerkers er meer mee bezig zijn. Vragen of bepaalde mailberichten wel veilig zijn, of bepaalde documenten wel gedeeld mogen worden. Behoorlijk praktisch dus, maar het gesprek dat erdoor ontstaat vind ik grote winst.'

Wat vraagt I-bewust werken van medewerkers in de praktijk?

Wendy: 'Dat medewerkers stilstaan bij de waarde van hun informatie. Deze informatie kan, naast het realiseren van eigen werkdoelen, van belang zijn voor anderen. Zowel binnen als buiten de organisatie neemt de productie van en het zoeken naar informatie toe. Het hebben van een goed netwerk, vaardigheden als het delen en hergebruiken van informatie (welke bronnen zijn wel/niet betrouwbaar, welke informatie is wel/niet relevant) worden steeds belangrijker. Een verandering in werkwijze is niet van gisteren op vandaag gerealiseerd. Dit is een proces met vallen en opstaan, met elkaar in gesprek gaan en elkaar helpen. I-bewustzijn is daarmee een samenspel.'
Hylke: 'Dat is zeker van belang. We kunnen namelijk nog zoveel technische maatregelen treffen, maar als het vervolgens niet wordt nageleefd blijven de risico's bestaan.'

Wat zouden jullie nog mee willen geven?

Wendy: 'Wat natuurlijk van belang is, is te onderkennen dat 100% veilig niet bestaat, maar dat we met elkaar wel het verschil kunnen maken.'
Hylke: 'Inderdaad. De technologische ontwikkelingen gaan heel snel, dat vraagt een continue aanpassing van mens en organisatie, en voortdurende aandacht. Verslappen is geen optie.'

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers

COLUMN

Bewustwording

In de I-strategie VenJ hebben we aangegeven dat de toenemende digitalisering van de samenleving een impuls is voor legale én illegale activiteit. Dat wij daarbij de taak hebben om Nederland te behoeden tegen bedreigingen die de maatschappij kunnen ontwrichten, dus is onze geloofwaardigheid in het geding wanneer we onszelf niet beschermen. VenJ heeft hier een voorbeeldrol te vervullen. Als ministerie van Veiligheid en Justitie hebben we beleidsmatig een coördinerende rol ten aanzien van cybersecurity, wat ons ook de verplichting geeft om het adagium goed voorbeeld doet goed volgen te hanteren.

Met de phishing actie van de afgelopen maanden, het programma voor de Alert Online campagne, dit magazine en het opstellen van een strategische nota iBewustzijn geven wij op meerdere manieren vorm en inhoud aan deze rol.

Bewustwording van ons allen is daarbij een eerste stap. Ik ik hoop dat jullie allemaal veel leesplezier hebben gehad.

Emine Özyenici
Directeur Informatisering & Inkoop VenJ

Feiten en cijfers phishing-campagne

Heb jij de twee phishing-mails in je inbox herkend en niet geopend? Goed zo! Dan hoor je bij de 88 procent die zich tijdens de phishing-campagne niet heeft laten verleiden. Twaalf procent van je 53.000 collega's heeft de phishing-mails wél geopend. Wie van je collega's de phishing-mails hebben geopend, of welke afdeling hoog of laag scoort, is niet bekend; alle data zijn anoniem. In de phishing-mail werd je verleid met drie lokkertjes. In de eerste e-mail kon je een cadeaubon ter waarde van 25 euro winnen. De tweede e-mail betrof een LinkedIn-uitnodiging. Er volgt nog een derde mail in het najaar. Wees dus alert! Als je op een link in de phishing-mail klikte, kwam je terecht op een speciale pagina met daarop de melding 'Oeps, je bent erin getrapt!', gevolgd door info en tips om een phishing-mail voortaan te herkennen. Voor dit deel van de campagne is samengewerkt met Veiliginternetten.nl. Daar vind je een speciale campagnepagina met info en tips en tricks om phishing te voorkomen: **www.veiliginternetten.nl/phishing.**

Achtergrond phishing-campagne

De phishing-campagne van het ministerie van Veiligheid en Justitie (VenJ) is in april gestart. Het is de aftrap van de iBewustzijn-campagne die VenJ aan het ontwikkelen, opzetten en uitvoeren is. In de iBewustzijn-campagne staat het bewustzijn rond informatieveiligheid centraal. De campagne en bijbehorende activiteiten zijn erop gericht om jou en jouw collega's te stimuleren en te ondersteunen zodat we met z'n allen bewuster en vaardiger worden als het om informatieveiligheid gaat. De iBewustzijn-campagne sluit aan bij de doelstellingen uit de Informatiestrategie 2017-2022 (I-strategie) van VenJ.

Colofon

Uitgave
Ministerie van Veiligheid en Justitie
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Hoofdredactie
Monique Barnhoorn,
Ministerie van Veiligheid en Justitie, Directie Informatisering & Inkoop

Annet van Veen,
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Directie CIO Staf

Tekst en eindredactie
Stijn Jaspers (Veiliginternetten.nl)

Fotografie
AVEQ
Stijn Jaspers (Veiliginternetten.nl)

Illustraties
CJIB
Veiliginternetten.nl

Vormgeving
Optima Forma bv

inhoud

- voorwoord
- phishing via smartphone of tablet
- interview Martijn Bouckaert
- zo herken je een phishing-mail
- interview Annet van Veen
- leestips
- programma overzicht
- column Mischa Rick van Geelen
- interview Ronald Barendse en Emine Özyenici
- interview Stijn Jaspers
- imago en huisstijl CJIB
- interview Wendy Sutherland en Hylke Wierda
- column Emine Özyenici
- feiten en cijfers