BUURTINFORMATIENETWERKEN EDEGEM –

27

Omdat veiligheid iedereen aanbelangt

Beste BIN-leden,

1. Feedback recente dringende BIN-berichten.

23/09/2015 22u34 BIN-Centrum

Verdacht persoon in de Victoriastraat. We hebben geen bijkomende informatie ontvangen.

2. Auto-inbrekers stelen airbags. (bron Het Laatste Nieuws)

EDEGEM 24/09/2015 - 03u12
In Edegem zijn auto-inbrekers tijdens de nacht van dinsdag op woensdag aan de haal gegaan met twee airbags. De daders sloegen toe in een Volkswagen Passat in de Hendrik Kennisstraat en een Mazda 5 in de Varenblok. De airbags werden bij beide wagens uit het stuur gehaald. Aan de buitenkant van de auto's waren geen inbraaksporen te vinden. De politie vond in de Passat wel een schroevendraaier van de daders. Er zijn geen getuigen van de inbraken. De politie spoort de daders op. Deze plaag blijft dus maar duren. Meldt onverwijld elk verdacht gedrag via **101**.

3. 1 dag niet.

De nationale actiedag van de strijd tegen inbraak **"1 dag niet"** is dit jaar vastgelegd op **vrijdag 13 november 2015**. Deze datum valt samen met het begin van de donkere maanden. De ideale gelegenheid om de burgers te sensibiliseren voor sociale waakzaamheid en het beveiligen van hun woning! Met de website 1DagNiet willen politiemensen in Nederland en België de bewustwording over het thema woninginbraken onder inwoners van vergroten, en daarnaast bijdragen aan sociale verbindingen in de wijk. De site zorgt ervoor dat we gaan nadenken over positieve initiatieven in of rond het eigen huis, straat of wijk.
Bezoek de website : 1dagniet.be
Als buurtinformatienetwerk gaan we ons steentje bijdragen. Wat het zal worden lees je in één van de volgende BIN-bulletins.

4. Valse verkeersboetes - Phishing in naam van de federale politie.

Ook een fenomeen waar men voor blijft waarschuwen. Hieronder een voorbeeld. Dit zijn duidelijke gevallen van phishing. Klik in geen geval op de links **en betaal niet**. Let op met dergelijke e-mails. De mails kunnen er soms een beetje anders uitzien maar de werkwijze van de oplichters blijft hetzelfde.

Politie Police

Geachte bestuurder,

Bij deze willen wij u mededelen dat u nog een bedrag bij ons heeft openstaan wegens het overtreden van een verkeersvoorschrift.
Hiervoor is een administratieve sanctie opgelegd. Wij hebben u al eerder per brief verzocht om de betaling te voldoen. Het openstaande bedrag is tot op heden niet op de rekening van het Federale Politie bijgeschreven.

Informatie over de overtreding en de opgelegde administratieve sanctie

Overschrijding maximum snelheid van 100km/h met 18km/h
Uw gereden snelheid na toepassing van de marge is 110.92

Datum overtreding	12 augustus 2015
Bedrag overtreding	€63,50
Buitengerechtelijke domiciliëringskosten	€40,00
Totaalbedrag te voldoen	**€103,50**

Daarom zien wij ons genoodzaakt u te sommeren om onderstaand bedrag, vermeerderd met de wettelijke en buitenrechtelijke kosten,
binnen 3 dagen te voldoen via 3V Payment Group.

Indien het openstaande bedrag niet binnen de door ons gestelde termijn is voldaan,
dan zult u door ons negatief worden geregistreerd, en zal het bedrag 2 maal vergroot worden.
En dan hebben wij het recht om uw rijbewijs in ons bezit te krijgen.

Klik hier om het openstaande bedrag te voldoen. Zodra het openstaande bedrag via 3V Payment Group is voldaan, ontvangt u via de email een unieke 19-cijferige code.

Klik hier om de 19-cijferige code in te vullen die u heeft ontvangen per email,
als u dat heeft gedaan ontvangt u binnen 3 dagen een bevestiging dat u heeft betaald.

Bancontact

5. *Alarmeringstest op 1 oktober 2015.*

Donderdag 1 oktober wordt een alarmeringstest uitgevoerd door het Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken.

Tussen 11.45 en 13.15 uur zal de trimestriële test van het netwerk van de 570 elektronische sirenes plaatsvinden. Deze sirenes zijn opgesteld rond nucleaire sites en Seveso-ondernemingen met hoge drempel. Het sirenenetwerk kan worden ingezet om de bevolking te verwittigen bij noodsituaties.
Als u een sirene hoort bij een noodsituatie, is de juiste reflex naar binnen te gaan of binnen te blijven en de aanbevelingen van de overheid te volgen, meer bepaald via de media.

De sirenes worden regelmatig getest om zeker te zijn dat ze werken bij een noodsituatie. Dagelijks wordt een stille test uitgevoerd, die niet hoorbaar is voor het menselijke gehoor. Elke eerste donderdag van het trimester wordt een hoorbare test gehouden.

Het alarmsignaal bij de trimestriële test is een gemoduleerde scherpe toon die na een korte onderbreking wordt herhaald. Na dit signaal weerklinkt de gesproken boodschap

"Proefsignaal". Tijdens de test duurt het alarmsignaal ongeveer 1 minuut. Bij een reële noodsituatie duurt het signaal ongeveer 3 minuten en kan het ook meermaals worden herhaald.
De bevolking kan informatie over deze alarmeringstests krijgen via het informatienummer 0800-94 113 in de week van de test. Inwoners kunnen hun opmerkingen ook meedelen via be-alert@ibz.fgov.be.

Alarmeringstesten in 2016

Ook in 2016 wordt elke eerste donderdag van het trimester een alarmeringstest gehouden.

6. *Enkele tips om uw PC te beveiligen tegen ongewenst bezoek* *(bron FOD Binnenlandse Zaken)*

Antivirus, firewall, spyware, maltase, spam, Trojaanse paarden, encryptie, Wep en Wap zijn niet uw ding? Niet elke computergebruiker is een krak in informatica. Dat hoeft ook niet zolang u maar een aantal elementaire zaken niet over het hoofd ziet.

Ben ik dan bedreigd?

Elke PC die aangesloten is op het internet loopt kans om aangevallen te worden. De vijand is meestal uit op het vernemen van vertrouwelijke gegevens of het aanrichten van schade. Er is veel kans dat u niet eens merkt dat een aanvaller via uw PC meeleest wat u intikt op het klavier. Ook een PC die niet is aangesloten op het internet kan het slachtoffer worden van een aanval (bijvoorbeeld via het lezen van informatie die op een USB-stick staat) maar die kans is veel kleiner.

Ja, maar kan ik er zelf iets aan doen?

Tip 1 : Doe uw PC een paswoord cadeau

Rust uw PC uit met een paswoord. Telkens als u de PC aanzet zal u gevraagd worden het paswoord in te voeren. Kies een paswoord dat niet eenvoudig te achterhalen is. Maak een zin die u gemakkelijk kunt onthouden en gebruik bijvoorbeeld van elk woord de eerste letter:

"ik hou zo van fietsen aan zee!" → paswoord: ihzvfaz!

Wat cijfers of leestekens opnemen in het paswoord maken het nog moeilijker om het te achterhalen.

Wijzig minstens maandelijks het paswoord (meer is beter). Uiteraard noteert u het paswoord niet. U laat uw autosleutels toch ook niet achter bij de wagen. Gebruik ook nooit hetzelfde paswoord voor uw kluis, uw elektronische identiteitskaart , uw bankkaart(en), … en uw PC.

Geef toekijkers geen kans om mee te lezen als u het paswoord intikt op het klavier. Moet u even weg van het klavier? Schakel dan de PC uit (of log uit).

Tip 2 : Hou het besturingssysteem up-to-date

Een besturingssysteem? Jawel, U hebt uw PC aangekocht met een "besturingssysteem" (OS of Operating System in het Engels). XP, Vista en Mac OS zijn bekende besturingssystemen. Zonder het besturingssysteem kan de PC niet werken. Zo'n besturingssysteem is nooit perfect en dat weet de vijand ook. Vele aanvallen kunnen plaatsvinden omdat het besturingssysteem zwakke plekken vertoont. De ontwikkelaars doen alle moeite om hun systemen voortdurend beter te beveiligen. Het is dan ook belangrijk steeds te beschikken over de recentste versie. Als u met het internet verbonden bent hoeft u daar meestal niets voor te doen. De updates gebeuren automatisch. Hoogstens krijgt u een waarschuwing en moet u toestemming geven. Voordat u toestemt loont het de moeite om te lezen welke aanpassingen uitgevoerd zullen worden en waarom. Die informatie wordt veelal samen aangeboden met de vraag om toestemming. Is er geen informatie beschikbaar dan is het aanbod twijfelachtig en kan u best weigeren.

Tip 3 : Vergewis u ervan dat u beschikt over een bijkomende bescherming

De meeste PC worden verkocht met een programma dat bijkomend bescherming biedt tegen aanvallen van allerlei aard. Bekende programma's zijn die van Symantec, AVG, Cyberdefender, Bitdefender, enz. Als u niet weet of u zo een programma hebt, kijk dan even naar de icoontjes rechts onderaan uw scherm. Plaats de loper (het symbool dat over het scherm beweegt als u de muis verplaatst) op de icoontjes om de naam van het bijbehorende programma zichtbaar te maken. Als u met de rechtermuisknop op het icoontje klikt kunt u het programma ook openen en krijgt u de mogelijkheid om de parameters in te stellen.

Maak u daarover geen zorgen want de parameters die ingesteld zijn bij de installatie door de leverancier bieden zeker voldoende beveiliging.

Zoals voor het besturingssysteem is een regelmatige update van het beveiligingsprogramma een absolute noodzaak om u te wapenen tegen de nieuwste bedreigingen. Gelukkig zorgen de ingestelde automatismen ervoor dat dit op regelmatige tijdstippen automatisch gebeurt. Wilt u zeker zijn: open dan het programma en bekijk de status.

Waarschuwing: bij de aankoop van de PC met beveiligingssoftware hoort meestal ook een abonnement voor het op peil houden van die software. Soms hebt u recht op een aantal maanden gratis service, maar daarna zal u gevraagd worden te betalen om de updates in de toekomst verder te ontvangen. Dat bedrag schommelt tussen de 50 en 100 euro. U kunt ook kiezen voor een gratis beveiligingsprogramma maar u mag daarvan uiteraard niet hetzelfde beveiligingsniveau of dezelfde service van de ontwikkelaar verwachten.

Tip 4 : E-mail en surfen

E-mail en surfen zijn ongetwijfeld de meest gebruikte toepassingen via het internet.

Open nooit e-mails waarvan de herkomst onduidelijk is. Verwijder ze onmiddellijk!

Vele websites, en in het bijzonder websites zoals die van banken, mutualiteiten en andere, die vertrouwelijke gegevens met u uitwisselen, maken gebruik van een "beveiligde" verbinding. Dat is te merken aan het adres van de website dat begint met "https" in plaats van "http".

Ga nooit in op vragen om vertrouwelijke gegevens (paswoorden, pincodes, namen, adressen, enz.) mee te delen als u niet zeker bent van uw stuk. De vijand weet immers maar al te goed hoe hij het moet aanpakken om vlot "mee te lezen". Hij weet ook hoe hij u een beeld kan voorschotelen dat sterk lijkt op dat van uw bank, mutualiteit enz. U zult het verschil alleen merken aan de details (één letter verschil in de naam van de bank, maar misschien denkt u dat het om een typefout gaat).

Tip 5 : Kijk, ik doe het zonder draad!

Draadloos werken biedt heel wat comfort. U werkt met uw laptop in de tuin, de keuken, … en dat allemaal zonder kabeltje tussen uw PC en de internetaansluiting. Geen probleem, zolang u er maar aan denkt om uw draadloze verbinding voldoende te beveiligen. Draadloze signalen kennen nu eenmaal geen grenzen. Het signaal dat uw PC uitzendt is waarschijnlijk gemakkelijk te onderscheppen door uw buurman, die als geen ander weet hoe hij uw PC moet binnendringen. U hebt het begrepen. Een goede beveiliging is hier op zijn plaats. Niet zo eenvoudig. Als u er zelf niets van kent doet u best beroep op uw verkoper of een specialist terzake.

Tip 6 : Een softwarepakket voor alles en voor niets

Het internet bevat een schat aan gegevens. Spoedig ontdekt u dat van het internet heel wat programma's afgehaald kunnen voor heel weinig geld. Verleidelijk! En dat weten de "indringers" ook. Ze maken dankbaar gebruik van hun software om uw PC te besmetten en zo achter uw persoonlijke gegevens te komen.

Veilige softwarepakketten van goede kwaliteit hebben nu eenmaal hun prijs. Leg dus de nodige argwaan aan de dag bij de aanbiedingen op het internet. Lees in elk geval steeds aandachtig de licentieovereenkomst voordat u de installatie start. Gaat u niet akkoord, stop dan de installatie van de software op uw PC.

Tip 7 : Uw eID beschermt. Maak er gebruik van

Er zit niet voor niets een chip op uw eID (elektronische identiteitskaart). Met uw eID kan u op afstand - bijvoorbeeld via het internet - bewijzen wie u bent en documenten tekenen.

Meer en meer websites en toepassingen, zeker als het toepassingen betreft die toegang geven tot vertrouwelijke gegevens, vragen te bewijzen wie u bent aan de hand van uw eID (men spreekt van authenticeren). U moet dan uw pincode intikken en het "authenticatiecertificaat" kiezen om dat bewijs te leveren.

Om uw eID te gebruiken met uw PC moet u beschikken over een kaartlezer en een stukje software, "middleware" genoemd. De "middleware" kunt u afhalen van de site http://eid.belgium.be. U vindt op die site ook een schat aan gegevens over hoe u met de eID e-mails en documenten kunt ondertekenen en over "authenticatie".

De kaartlezer is meestal ingebouwd in het klavier van uw PC. Externe kaartlezers worden met uw PC verbonden via een USB-poort. Externe kaartlezers die beschikken over een eigen klavier zijn het veiligst. U tikt dan de Pincode van uw eID in op het klavier van de kaartlezer, dat volledig los staat van de PC. Meelezen kan dus niet.

Koester uw eID alsof het uw bankkaart was. Laat uw Pincode nooit aan iemand anders zien, en wijzig ze af en toe eens! Dat kan u doen met de middleware. Verwittig bij verlies of diefstal onmiddellijk de dienst DOCSTOP via het gratis nummer **00800 2123 2123** (jawel **twee maal nul** achthonderd enz.). Informatie over wat te doen bij verlies of diefstal vindt u ook op deze website: http://www.ibz.rrn.fgov.be/nl/faq/identiteitsdocumenten/eid/.

Tip 8 : Teken ik wel het document dat ik op mijn scherm zie?

Een terechte vraag. Met de eID tekent u een digitaal document (een reeks enen en nullen), en dat zit in het geheugen van uw PC. Het programma (Word, Excel, Acrobat, …) dat u gebruikt transformeert het digitale document naar de afbeelding op het scherm. Maar staat het wel vast dat het om hetzelfde document gaat?

Alleen de ontwikkelaar van het programma kan dat garanderen. Men heeft het over WYSIWYS of "what you see is what you sign". Alweer een reden om geen illegale of bedenkelijke softwarepakketten te gebruiken.

Tip 9 : Een dosis argwaan is gezond

Gezond voor u en uw PC. Ga nooit in op vragen naar persoonlijke gegevens (naam, adres, telefoonnummers, geboortedatum, Pincodes, paswoorden, nummers van bank- en kredietkaarten, …), zelfs al lijken ze te komen van een website, of via een mail, die u op het eerste zicht vertrouwen schenkt. Personen die dergelijke zaken willen vernemen via het internet menen het meestal niet zo goed.

7. Voor deze 57 malafide bedrijven moet u uitkijken. (Bron FOD Economie)

De Federale overheidsdienst (FOD) Economie heeft een nieuwe lijst met 57 namen van verdachte firma's vrijgegeven. Zo kregen veel bedrijven en zelfstandigen de afgelopen maanden een brief en een rekening in de bus met het verzoek de domeinnaam van hun website dringend te betalen. 'Pure oplichting', aldus de FOD Economie.

'Een van de malafide bedrijfjes waarvoor we waarschuwen is BE Domein Host', een spookfirma die vermoedelijk vanuit Spanje opereert en dit jaar al goed is voor meer dan 300 klachten', zegt Johan Verbelen van de FOD Economie.

'Ze bellen bedrijven op en vragen om dringend hun domeinnaam op het internet te betalen. Anders zou die wel eens door anderen kunnen worden gekocht en kan hun imago geschaad worden. Vaak hebben de aangeklampte firma's al een internetsite die eindigt op de extensie .be, maar stellen ronselaars hen voor ook de extensies .biz, .net en .name te kopen om te vermijden

dat er verwarring zou ontstaan met andere firma's met een soortgelijke naam. Bij de tweede methode sturen ze ook vaak een factuur met de vermelding 'herinnering'. Deze factuur zet mensen er meestal toe aan om zo vlug mogelijk te betalen zonder na te gaan of ze terecht is, omdat het meestal om relatief kleine bedragen gaat', zegt Johan Verbelen.

In 2014 ontving de FOD Economie 210 klachten over bedrog met domeinnamen. Dit jaar waren dat er al 124 meldingen en in bijna alle gevallen ging het om BE Domein Host. Het bedrijf dat vermoedelijk vanuit Spanje opereert, is een van de 57 bedrijfjes dat op de zwarte lijst staat die de FOD Economie op haar site heeft geplaatst.

Reclameronselaars

Fraude met domeinnamen is een vrij recent fenomeen . Valse reclameronselaars bestaan al langer. 'Die ronselaars komen langs met het voorstel om reclame voor uw onderneming op te nemen in een catalogus die in de regio verspreid wordt ten voordele van goede doelen. In de meeste gevallen is dat goede doel echter twijfelachtig of bestaat het zelfs niet', zegt Verbelen.

Of u krijgt een brief waarin men u verzoekt de adresgegevens van uw onderneming te corrigeren met het oog op een bijwerking van een databank of gids. Men vraagt u het document te ondertekenen en terug te sturen. Maar wanneer u dit document ondertekent, bent u gebonden aan een buitensporig duur contract dat pas 2 of 3 jaar later afloopt. Bovendien krijgt u er maar een middelmatige dienstverlening of helemaal niets voor.

De Economische Inspectie ontving vorig jaar 969 van dergelijke klachten, iets minder dan het jaar voordien. Voor de eerste helft van 2015 waren dat er 325.

Tips

De FOD Economie geeft enkele tips mee voor wie met malafide bedrijven in contact komt.

'Wij raden mensen aan nooit een twijfelachtig aanbod te tekenen, ook al komt de verkoper u vriendelijk en betrouwbaar over. Betaal ook geen factuur waarop 'herinnering' staat zonder vooraf goed te controleren of er geen sprake is van oplichting. Bent u toch opgelicht, stap dan naar de politie en dien dan ook een klacht in bij de FOD Economie', zegt Verbelen.

Lijst van verdachte maatschappijen

- European trademark publications (ETP)
- Adressengids Vlaanderen
- BE Domein Host
- Best Print
- BMS / XL Media
- BPS (Belgium Packet Service)
- Call Center Vlaanderen BVBA
- Construct Data
- Custom Contact Nederland (bedrijvenonline.nu)
- DAD - Deutscher Adressdienst / Registre Internet belge
- DND BVBA
- Drukkerij Rubrecht
- Easy Pages Ltd / European www register
- Edition Hekking Cornélis

- EMS European Marketing Service - Pages Jaunes Belgique
- Euro Business Guide
- Euro Media Conseil / Ema Web Vision
- Euroguide.de
- European City Guide
- Expo Guide
- Firma Mareel
- Gele-gids.com
- GCS - Global Call Services
- Global Earth Register
- Globe Trade Control
- Guide pour la ville
- IBR International Business register - Pages Jaunes Belgique
- Index-Entreprise / Etude Grivière SAO France
- Inet Biz Solutions
- Intercable Verlag
- IRD
- MCF - Services des Professionels
- MCH Printing Services / International Publicity Services (IPS)
- Media Belgique Design
- Media Connect
- Media Group Vlaanderen
- Media Print
- Media Service AS
- Media Service Verlag
- Nederland Media Register
- Nieuwe Bedrijvengids / Belga Marketing / Internet Bedrijvengids / Annuaire pro / Bedrijvengids Belgie
- Pan World Life
- Print Media Group / Plattegrond *(Let op : mag niet verward worden met PrintMedia Group uit Genk, een onderneming die weliswaar bijna dezelde naam draagt, maar niets te maken heeft met reclameronseling)*
- Publi Trends
- Registre des Branches professionnelles
- Service-pro / Eurl Media Press
- TM - Collections
- TVV - Tele Verzeichnis Verlag / Ondernemings Portaal
- Uitgeverij Vilain
- United Lda / Nova Channel / Temdi / Med1web
- Unitel Nijmegen B.V.
- Webdirect
- World Business Guide
- World Company Register / World Company Directory
- WZD - Wolf SW / Banque Centrale des données économiques
- Yellow-Pages
- Zoom Trends SL