



Nieuwsbrief BIN Hey-End

Uitgever

Bestuur BIN Hey-End

Juni 2010

Nummer 10/02

Veranderingen in het ledenbestand

Nieuw lid: Rudi, Sandi, Kelly en Nikki **Steegmans**, Eikenblok 16.
We zijn nu met 228 leden.

Zorgenvrij met vakantie

(laat de Politie weten dat U weg bent en verzeker U van extra toezicht)

Een aanvraagformulier voor vakantietoezicht kan u downloaden van de website BIN Hey-End of via de website gemeente Essen – rubriek politie . Voor de leden zonder email adres voegen we een blanco toe aan de Nieuwsbrief. Dit document kan u ook uiteraard gratis ophalen aan de balie van het politie kantoor .

Feilloos Uw weg vinden met een GPS-systeem

(maar bent U de enige die de weg naar Uw huis vindt?)

Van BIN-Kijkuit: Wees voorzichtig met het gebruik van je GPS: Steeds meer mensen gebruiken een navigatiesysteem om op de plaats van bestemming te komen. Zo ook inbrekers natuurlijk! Stel u even het volgende voor: een familie gaat met de auto op vakantie naar een bungalowpark. Ze hebben net een leuke dagtrip gemaakt. Ze laten hun auto op de parking, om in de kantine een frisse consumptie te gebruiken. Wanneer ze terug naar hun bungalow willen vertrekken, merken ze dat hun GPS toestel gestolen is. Later op die avond worden deze mensen gebeld door de bureaus (thuisfront). Hun huis werd bezocht door inbrekers! De inbrekers zijn, via de functietoets “THUIS”, simpelweg naar de woning van de eigenaars genavigeerd. Ze weten immers dat deze niet thuis zijn en dat ze ongestoord hun slag kunnen slaan. Dus, toets in je navigatiesysteem onder “THUIS” nooit je eigen huisadres in. Dit adres ken je zelf goed genoeg. Toets bvb. het adres van het politiebureau in je gemeente in. Wanneer je navigatietoestel gestolen is, blijft het hierbij. De dieven weten nu toch niet waar je woont. Het beste is natuurlijk je GPS niet in de auto achter te laten!!!

Gratis advies huisbeveiliging

(de enige oprechte en betrouwbare adviseur: de Politie)

Het aanvraagformulier voor Technopreventief advies kan u ook downloaden via de

[website gemeente Essen – rubriek politie](#) . Voor de leden zonder een email adres voegen we eveneens en blanco document toe aan de Nieuwsbrief .

Wij krijgen na een BIN-oproep wel eens reacties van BIN-leden die zich beklagen over de 'weinig' info die zij krijgen via de ingesproken boodschap van de dispatcher. In de meeste gevallen bij een heterdaad woninginbraak, is er (gelukkig) geen visueel contact tussen de bewoners en de inbreker. De bewoners/oproeper kunnen dus zelf weinig informatie geven als zij de politie opbellen omdat ze zelf niets of nauwelijks iets gezien hebben. De dispatcher kan dus evenmin informatie over de inbrekers vermelden in zijn boodschap!

Dit is trouwens ook niet de bedoeling van een BIN-oproep: van de BIN-leden wordt niet verwacht dat zij zelf op onderzoek uitgaan of voor RAMBO gaan spelen. De BIN-oproep heeft tot doel de mensen te waarschuwen hun verlichting aan te steken en alert te zijn om zo te voorkomen dat die inbreker in dezelfde straat of dezelfde buurt opnieuw gaat inbreken!

Mensen bellen na een oproep ook wel eens naar de politie om te vragen hoe lang hun buitenverlichting moet blijven branden en/of de daders al gepakt zijn. Op dergelijke vragen kan meestal geen antwoord gegeven worden en voor de dispatchers betekent dit een bijkomende werklust.

De algemene regel is dat de BIN-leden hun buitenlicht laten branden tot zij 's morgens opstaan en/of het licht is. Als er inderdaad inbrekers gepakt worden, wordt dat nadien gecommuniceerd naar de BIN-besturen die dat dan kunnen doormailen aan hun leden!

[Het volgende geldt niet specifiek voor onze BIN maar heeft algemene geldigheid:](#) in december 2009 werden woninginbraken opvallend veel vastgesteld overdag. Meer bepaald waren er 'inbraakpieken' op: dinsdag tussen 11u00 en 14u00 , woensdag tussen 10u00 en 12u00 , vrijdag tussen 17u00 en 21u00 en zaterdag tussen 16u00 en 21u00.

Dit betekent uiteraard niet dat de andere tijdstippen verwaarloosbaar zijn maar het toont wel aan dat inbraken niet exclusief 's nachts gebeuren. Iedereen dient dus alert te zijn en de woning goed af te sluiten, ook overdag!!!

Recentelijk heeft de politie twee inbraken vastgesteld waarbij de daders via het dak binnengedrongen zijn door een gat in het dak te maken of een raam in te slaan met behulp van een dakpan. Hier sta je vrij machteloos tegenover.

Geen ladders of ander klimtuig laten rondslingeren is een optie; waakzaamheid voor de hele buurt eveneens!!! Verdachte voertuigen en personen steeds melden aan de politie: hoe meer wij die personen kunnen controleren, hoe sneller ze uit uw BIN-zone verdwenen zijn!

En dan Uw auto

(centrale vergrendeling – bron: Test Aankoop juni 2010)

[\(We verwijzen ook naar onze specifieke toegezonden BIN Flash 04 / 2010 in verband met afsluiten van auto's. Wees ook alert met een huurauto tijdens uw verlof, verwijder desnoods de reclamekaart of kenmerken van de verhuurfirma aan uw binnenspiegel\).](#)

- De eerste systemen voor centrale deurvergrendeling werkten vaak met een infrarood signaal en een unieke code, die vrij makkelijk te achterhalen was;
- Sindsdien gebruiken alle constructeurs een van de drie elektronische systemen die op de markt zijn en die allemaal werken met versleutelde protocollen;
- Een testlab heeft aangetoond dat de code van een van die systemen te kraken viel, maar

- dat zelfs specialisten met geavanceerde apparatuur hier ruim een uur voor nodig hebben;
- De apparatuur en de kennis die daarvoor vereist zijn, liggen niet binnen het handbereik van "ordinaire" dieven;
 - Ook de statistieken wijzen niet op een toename van het aantal autodiefstallen, integendeel;
 - Uit voorzorg laat u beter geen waardevolle spullen zichtbaar achter in uw wagen. (maar dat laatste wist u al langer).

En verder:

In enkele aanpalende politie-zones werden tijdens een nacht verschillende diefstallen uit voertuigen gepleegd. Daarbij werd telkens een zijraam stuk geslagen.

Wij adviseren u het volgende:

- uw voertuig op een meer veilige plaats parkeren (op de oprit of in de garage in plaats van op de openbare weg);
- alarm van uw voertuig in werking stellen als het er mee uitgerust is;
- geen waardevolle voorwerpen in de auto achterlaten;
- boorddocumenten dagelijks mee naar binnen nemen

En Uw financiën

(hoe oplichters trachten toegang te krijgen tot Uw bankcode, creditcard, etc., door phishing)

Bronnen: www.soweb.be/veiligheid/

Phishing is een vorm van zwendel waarmee de oplichter probeert je persoonlijke gegevens zoals je bankcode, visakaartnummer, enz...te verkrijgen.

Op de site van Microsoft staat ook veel uitgelegd en ook worden tips gegeven hoe je jezelf zo goed mogelijk kunt beschermen tegen allerlei vormen van computercriminaliteit : <http://www.microsoft.com/belux/nl/protect/yourself/phishing/faq.msp>

Tenslotte: een site van de Belgische overheid met informatie over computercriminaliteit: <http://www.belgium.be/nl/justitie/veiligheid/criminaliteit/computercriminaliteit/internetfraude/>

Phishing gebeurt op een zeer slinkse wijze. Je ontvangt een professioneel uitziende e-mail, vaak met echt bestaande logo's van bankinstellingen of bekende Internet bedrijven. De inhoud is een gefantaseerd verhaal over een storing in het computersysteem, het ontdekken van misbruik van je bankkaart, de melding dat je een groot bedrag hebt gewonnen, het aanbieden van een reeks goederen aan uitzonderlijk goedkope voorwaarden..... Maar op het eind van het verhaal verzoekt men je om je persoonlijke gegevens door te sturen zoals pincodes, rekeninginformatie, wachtwoorden, bankkaartnummers.

Om het je makkelijk te maken hoef je vaak maar op een snelkoppeling te klikken die je naar een wederom "vertrouwd" uitziende pagina brengt waar je netjes alle gevraagde informatie kan invullen.

Deze phishing techniek blijkt een zeer winstgevende zaak te zijn want het aantal phishing-aanvallen is met 60% gestegen. Volgens recente schattingen trapt ongeveer 5% van de ontvangers van dit soort valse berichten in de valkuil. Je hoeft ook geen computer-expert te zijn om op deze manier iemands vertrouwelijke gegevens te achterhalen. Websites kunnen makkelijk nagemaakt worden en logo's kan je zo meteen kopiëren via de website van het bedrijf. Zie je het niet meteen zitten, dan kan je zelfs een phishing-kit gratis downloaden van Internet.

Hoe voorkom ik slachtoffer te worden van phishing ?

- Logisch wantrouwen: geen enkele bankinstelling of Internet-bedrijf speelt jouw gegevens zomaar kwijt en zal die ook nooit per e-mail opvragen;
- Reageer nooit op dergelijke berichten en verwijder ze meteen;
- Update je Internet Explorer: in de oudere versies kon het frauduleus adres makkelijk verborgen worden in de adresbalk;
Dit is een voorbeeld van een echt bestaande adres : www.ebay.com
En dit is een voorbeeld van een verdacht adres:
`www.ebay.com%1@www.xxxxxxxx.org`
Maar oudere browsers kunnen % en alles wat erachter staat niet tonen.
- Controleer het certificaat. Banken en internetbedrijven maken gebruik van beveiligde websites. Je herkent ze aan het adres dat begint met https i.p.v. http;
- Als je op een beveiligde pagina werkt zie je onderaan rechts in je statusbalk een slotpictogram. Als je op dit pictogram dubbelklikt kun je de certificaatinformatie controleren. Een certificaat is een verklaring waarin de identiteit van het bedrijf of de beveiliging van de website wordt bevestigd;
- Controleer van wie het email-bericht afkomstig is: klik met je rechtermuisknop op het e-mailbericht en kies: opties. Het return path is makkelijk te vervalsen. Maar het is veel moeilijker om het Received From te vervalsen.

Onthoud echter 1 ding: de veiligste verbinding is geen verbinding. Met andere woorden ben je verbonden met Internet dan loop je risico's

Internetcriminaliteit via de telefoon

Bron: een grote internationale bank)

Internetcriminelen nemen telefonisch contact op met klanten van banken. De criminelen doen zich voor als medewerkers van de bank, om op deze manier uw pincode of inloggegevens voor Internet Bankieren te stelen. **Geen enkele bank zal u vragen om uw inloggegevens of pincode. Niet telefonisch, niet via e-mail en niet in een pop-up-scherm.**

Bij elke bank wordt altijd zorgvuldig met uw persoonlijke informatie en veiligheid omgegaan. Geef nooit uw codes voor Internet Bankieren aan derden. U loopt hierbij het risico dat persoonlijke gegevens in handen komen van criminelen en er frauduleuze transacties plaats kunnen vinden. □□Mocht u telefonisch, via e-mail of op een andere manier benaderd worden om vertrouwelijke informatie te verstrekken, maak daarvan dan melding met [dit formulier](#). Om geen slachtoffer van [phishing](#) (zie eerder in deze Nieuwsbrief) te worden, kunt u maatregelen treffen.

Advies: 3x kloppen

Banken voldoen aan strenge beveiligingsstandaarden om ervoor te zorgen dat u uw financiële transacties ook online met vertrouwen kunt doen. Internetbankiert u veilig?

1. Klopt uw pc-beveiliging?

Elke bank doet er alles aan om haar website optimaal te beveiligen. Maar ook de beveiliging van uw pc moet in orde zijn.

Bescherm uw computer tegen virussen en spyware. Maak gebruik van recente

antivirussoftware en een firewall en zorg dat deze actief wordt als u uw computer aanzet. Zorg ervoor dat uw draadloze netwerk beveiligd is. Controleer regelmatig uw software en of u de nieuwste versie van uw internetbrowser gebruikt.

2. Klopt de website van uw bank?

Als u inlogt op de bank website, gaat dat automatisch via een beveiligde internetverbinding. Fraudeurs proberen de beveiliging te omzeilen door u naar een imitatiewebsite te leiden. Kijk of uw browser voldoet aan [alle veiligheidskenmerken](#).

3. Klopt de betaling?

Controleer altijd voor de zekerheid uw rekeningoverzicht. Check onder meer de bij- en afschrijvingen, de opgegeven bedragen, namen van begunstigen en hun rekeningnummers.

Het nieuwe bestuur per 1 maart 2010

(een paar nieuwe gezichten)

Zoals reeds eerder aangekondigd wenst **Petra De Wint** ontslag te nemen als coördinator. Vooreerst nogmaals mijn dank aan Petra voor de inzet en betrokkenheid sinds de opstart 01/12/2007. Petra blijft wel fungeren als straatverantwoordelijke van de Kalmthoutsesteenweg in de toekomst .



Het verheugt me als BIN Hey – End coordinator U haar vervanger te kunnen aankondigen. Na recent overleg en onderhoud heeft ons huidig Bin lid **Fred Schenkelaars** , wonende Eikenblok 39 aanvaard om deze functie waar te nemen vanaf 01 / 03 / 2010. Fred heeft ook toegezegd om desgevallend ondersteuning te geven voor Nieuwsbrieven.

Dit spontaan akkoord resulteert in een gedreven medewerker om aldus de taak van Petra & Clara over te nemen in de toekomst en te bestendigen. Gelet op het feit dat **Clara Kint** haar ontslag heeft aangeboden tezamen met Petra, was het noodzakelijk om extra ondersteuning te zoeken en voor deze redactie taken vervangers te vinden. Uiteraard ook dank aan Clara voor de vrijwillig geleverde inspanningen, zij blijft ook fungeren als straatverantwoordelijke van de Huybergsebaan in de toekomst.

Clara heeft ook de medewerking ivm informatica beheer stopgezet . Ons BIN lid **Bert Drost** , Eikenblok 35 heeft spontaan en op vrijwillige basis zijn medewerking toegezegd om de informatica verantwoordelijkheid op zich te nemen. Bert is op dit ogenblik reeds gestart met verschillende proef “ updates“ van onze BIN Heyend website en heeft reeds alternatieve voorstellen geformuleerd om te implementeren.

Fred en Bert, van harte welkom in het team.

De nieuwe gezichten zonder de “oude” te vergeten

Fred Schenkelaars – co-coördinator	Bert Drost - informaticus
 A portrait of Fred Schenkelaars, an older man with short grey hair and glasses, wearing a plaid shirt. He is looking directly at the camera with a neutral expression.	 A portrait of Bert Drost, a man with short dark hair, wearing a blue button-down shirt over a white t-shirt. He is smiling and looking slightly to the right of the camera.
<p>Eikenblok 39 Tel. 03-6771125 E: fred.schenkelaars@telenet.be</p>	<p>Eikenblok 35 Tel. 03-2338681 E: B.drost@ced-holding.nl</p>