BIN-Kammenstraat

BIN-FLASH

23-12-'21

NR 14 Voor BIN KAMMENSTRAAT en OMGEVING

(Grensstraat-Handelsstraat-Hemelrijklaan-Hemelrijkweg-Hondsberg- Hraditskostraat-Kammenstraat-Kloosterstraat-Lazaret- Schepen Veraartstraat-Schuurblok-Statievelden-Witzenbergstraat-Essen Oldenburgstraat)

Noodnummer: 101 of **112** of **03/620 29 29** (zie ook: www.binkammenstraat.be)

Rekeningnummer voor BIN-lidmaatschap: **BE79-7795-9630-7433** (info: 0475/74.50.37)

Beste Buurtbewoner,

We wensen je fijne feestdagen en een gelukkig, gezond en veilig nieuwjaar. Bedankt voor je inzet. Samen dienstbaar, samen zorgzaam, samen veilig, samen vooruit.

Opgelet! In Essen is er een leurder actief die zich voordoet als een medewerker van de gemeente Essen en zogenaamd geld ophaalt voor kansarme kinderen. Hij verkoopt spullen van winkelketen Action. Bij weigering komt de man agressief over. Politiezone Grens is op de hoogte.
Indien U bezoek krijgt van deze persoon , gelieve dit te melden aan Politie Zone Grens via **101** 0f **03/620 29 29**

Daarnaast willen we nog even het anoniem meldpunt www.drugsplantageontdekt.be vermelden.
Het Openbaar Ministerie, de politiediensten en de gouverneur van de provincie Antwerpen werkten samen om dit anoniem meldpunt in het leven te roepen in de gezamenlijke strijd tegen illegale drugsproductie en de schadelijke gevolgen ervan. Illegale drugsproductie kan erg gevaarlijke situaties en overlast veroorzaken. Dat stellen we helaas ook in de provincie Antwerpen steeds vaker vast.
Zo kan er bijvoorbeeld brand ontstaan in een woonwijk door een cannabisplantage, een explosie in een drugslab. Wandelaars of spelende kinderen kunnen tijdens een boswandeling stoten op chemisch afval. De gevolgen kunnen ernstig zijn, zowel voor toevallige voorbijgangers, hulpverleners als voor de directe omgeving en het milieu.
Op de website www.drugsplantageontdekt.be vind je alle informatie over verdachte elementen rond cannabisplantages, labo's en het dumpen en lozen van chemisch afval. Wie deze verdachte elementen of situaties opmerkt kan er volledig anoniem melding van maken via een online formulier.

Pas op voor valse vaccinatie-uitnodigingen

Nu er weer mensen een uitnodiging krijgen voor een herhalingsprik, stijgt ook het aantal meldingen van mensen die een valse oproep in hun mailbox kregen. De mails lijken heel goed op een echte uitnodiging, maar leiden naar een website waar je bankgegevens moet invoeren.

De vaccinatie en het vaccin zijn gratis. Er wordt niet gevraagd naar persoonlijke gegevens.

Geef dus geen paswoorden, pincodes of rekeningnummers. Je ontvangt de uitnodiging ook via de post en in 'mijn burgerprofiel'.

Hoe herken je een officiële uitnodiging voor de coronavaccinatie?

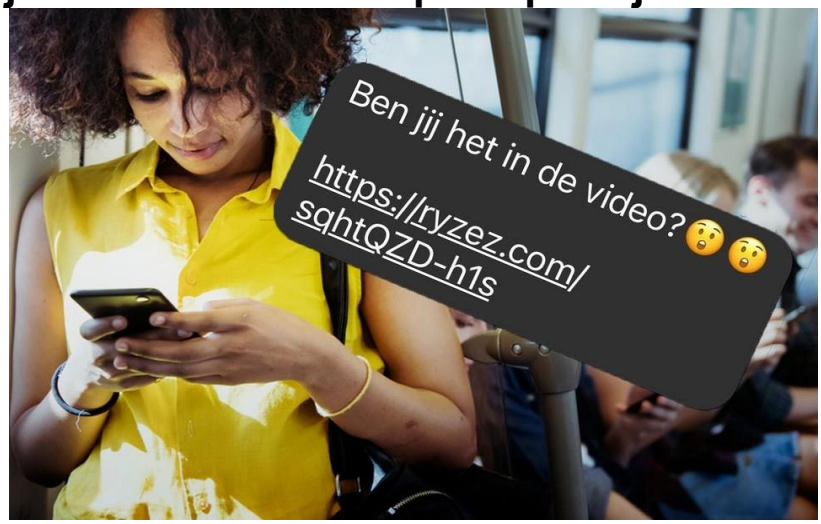
- Controleer de afzender. De uitnodiging ontvang je per mail van cov19-vaccin@doclr.be.
  Een sms krijg je van het nummer 8811.
- De uitnodiging vermeldt de contactgegevens van het vaccinatiecentrum in je regio.
  Jouw uitnodiging is persoonlijk en dus gelinkt aan je woonplaats.
- We vragen nooit persoonlijke gegevens zoals paswoorden, pincodes of rekeningnummers.
- We vragen nooit om een betaling of je bankgegevens: de vaccinatie en het vaccin zijn gratis.
- Je krijgt je persoonlijke uitnodiging ook altijd per post. Die valt enkele dagen na je digitale uitnodiging in de bus.

Stuur een verdacht bericht altijd onmiddellijk door naar verdacht@safeonweb.be.

Je kan ook afbeeldingen van een vals bericht doorsturen.

- Login of registreer om te kunnen reageren

“Ben jij het in die video?”: pas op als je dit berichtje krijgt



De jongste dagen circuleert er weer een venijnig virus dat via sociale media wordt verstuurd. Jij krijgt een mailtje waarin wordt gevraagd of jij dat bent in die video waarvan de link zogezegd wordt meegestuurd. Wie verder klikt, haalt het virus binnen.

“Ben jij het in de video” of de Franse versie “C’est toi dans la vidéo?” circuleert weer volop. Het zijn van die virussen die komen en gaan. Eens ze goed gekend zijn, verdwijnen ze. Om soms een hele tijd later weer op te duiken”, klinkt het bij Safeonweb, de cybersecurity van de overheid.
Het bericht komt meestal via messenger en is zogezegd verstuurd door een van je Facebookvrienden. De titel ‘Ben jij het in deze video?’ maakt mensen natuurlijk nieuwsgierig zodat ze willen gaan kijken naar de video.
“Als je op de link klikt, word je naar een valse webpagina geleid die naar je Facebook logingegevens vraagt. Als je je gegevens daar invult, zijn ze in handen van cybercriminelen die je Facebookaccount hacken en het bericht opnieuw doorsturen naar al jouw contacten”, zeggen experts die volgende tips geven.
Heb je dit bericht gekregen? Klik niet op de link naar de video en vul zeker geen gegevens in.
Stuur een afbeelding van het bericht door naar verdacht@safeonweb.be.
Verwittig je Facebookvriend van wie jij het bericht kreeg dat zijn of haar account gehackt is.

Heb je je gegevens doorgegeven?

Verander onmiddellijk je wachtwoord en stel tweestapsverificatie (2FA) in.
Waarschuw je contacten dat je gehackt bent en dat ze een vals bericht van jou kunnen verwachten.

Politie en parket waarschuwen voor RAT-fraude: “Slachtoffer raakte 183.000 euro kwijt”

De politie en het Antwerps parket waarschuwen opnieuw voor een gewiekste vorm van online oplichting. Deze keer gaat het om de zogenaamde RAT-fraude. Daarbij loggen criminelen vanop een afstand in op de computer van het slachtoffer, om zo geld te stelen. Vaak gaat het om grote bedragen. Recent deed een slachtoffer zelfs aangifte voor de diefstal van 183.000 euro.

Bij RAT-fraude wordt het slachtoffer in eerste instantie opgebeld door de oplichters. “Ze beweren een medewerker te zijn van een betrouwbare organisatie zoals de bank, de politie, Microsoft of Google en melden dat het geld van het slachtoffer niet veilig is”, legt woordvoerder Kristof Aerts van Antwerps parket uit.

De zogezegde medewerkers willen het slachtoffer helpen door snel toegang te krijgen tot hun computer. “Daarbij maken ze gebruik van hulpprogramma’s waarmee ze op afstand kunnen inloggen op andere computers, zogenaamde Remote Acces Tools (RAT). Met die programma’s beweren ze bijstand te bieden om geld veilig te stellen of bij geven ze hulp bij beleggingen met bijvoorbeeld cryptovaluta”, aldus Aerts.

Vrijgeleide naar je bankgegevens

In de praktijk krijgen de criminelen zo een vrijgeleide naar de bankgegevens van het slachtoffer en kunnen ze zo geld overschrijven vanop de rekeningen. Het Antwerps parket zag de laatste maanden een toename van het aantal aangiftes. “Vaak gaat het om grote bedragen. De recentste aangifte was van 183.000 euro nadeel. Er lopen nog enkele dossiers”, zegt Aerts. Daarom waarschuwen politie en parket nu nogmaals voor deze gewiekste vorm van oplichting.

Bescherm je gegevens

Hoe kan je best voorkomen dat je het slachtoffer wordt van RAT-fraude? Belangrijk is om altijd en overal je eigen bankgegevens te beschermen. “Een bank zal nooit vragen om software te downloaden en installeren of geld tijdelijk over te zetten naar een zogenaamde veilige rekening”, waarschuwt het parket. “Het is bovendien nooit een goed idee om mensen op afstand toegang te geven tot je computer als je bankverrichtingen aan het uitvoeren bent.”

Wie toch het slachtoffer is geworden van RAT-fraude, krijgt de raad zo snel mogelijk aangifte te doen bij de politie en bij de bank om zo te proberen de financiële transactie te laten blokkeren. Verzamel ook zo veel mogelijk relevante informatie en geef dit door aan de politie.

Bron: Het Nieuwsblad

Ook volgende mail is FRAUDULEUS: indien je zo eentje zoals hieronder, binnenkrijgt, zend deze dan door naar: verdacht@safeonweb.be en verwijder de mail.

Van: service@proximus.com <no-reply@online-diyshow.com>
Verzonden: dinsdag 21 december 2021 23:09
Aan:
Onderwerp: Mise à jour requise.

Chèr(e) client(e),

Nous vous informons que votre mode de paiement a été refusé.

Merci de mettre à jour vos informations de facturation pour le prélèvement prévu le **26/12/2021** au plus tard.

Si vous n'effectuez pas la mise à jour avant de **26/12/2021** votre compte Proximus sera définitivement fermé et un montant de **59,99€** vous sera facturé suite aux frais de clôture de votre compte.

Consultez et réglez vos moyens de paiement très facilement dans MyProximus.

Als u niet update tegen 26/12/2021, wordt uw Proximus-account permanent gesloten en wordt u een bedrag van € 59,99 aangerekend na de kosten van het sluiten van uw account.

Raadpleeg en pas uw betaalmethodes heel gemakkelijk aan in MyProximus.

Mettre à jour

Laat niet zomaar vreemden binnen! 4 dagen geleden Criminaliteit, Essen, Nieuws Gisteren zijn er in de buurt van de Kloosterstraat mensen aan de deur geweest, die zich voordeden als medewerkers van Telenet om het modem van bewoners te bekijken. Geliefde periode voor inbrekers Navraag bij Telenet leerde echter dat er geen meldingen van storingen zijn geweest of dat er afspraken waren gemaakt. Ook werd verteld dat er zo al meer meldingen zijn binnengekomen. Het kan een manier zijn om te kijken of iemand thuis is, vooral als het een straat betreft met veel geparkeerde auto's, of binnen te komen om te kijken of er iets te halen valt. Dit zijn de donkere dagen voor Kerst en een zeer geliefde periode voor inbrekers. Wees en blijf dus voorzichtig, laat niet zomaar een onbekende binnen zonder dat die zich heeft gelegitimeerd, vooral als deze persoon zonder afspraak of vooraankondiging langskomt!

Bron: https://www.noordernieuws.be/laat-niet-zomaar-vreemden-binnen/

Wensen

● **Wees discreet op sociale media over je vakantie**.
Let ook op met antwoordapparaten en automatische e-mailberichten.
Nog meer tips vind je op de website www.besafe.be

BIN : SAMEN VEILIG !

Samen staan we sterk !
101 – 112 – 03/620.29.29.
B
POL I TIE
N

Met vriendelijke groeten,
Uw BIN-bestuur van KAMMENSTRAAT EN ZIJSTRATEN.