Cybercrimeinfo.nl

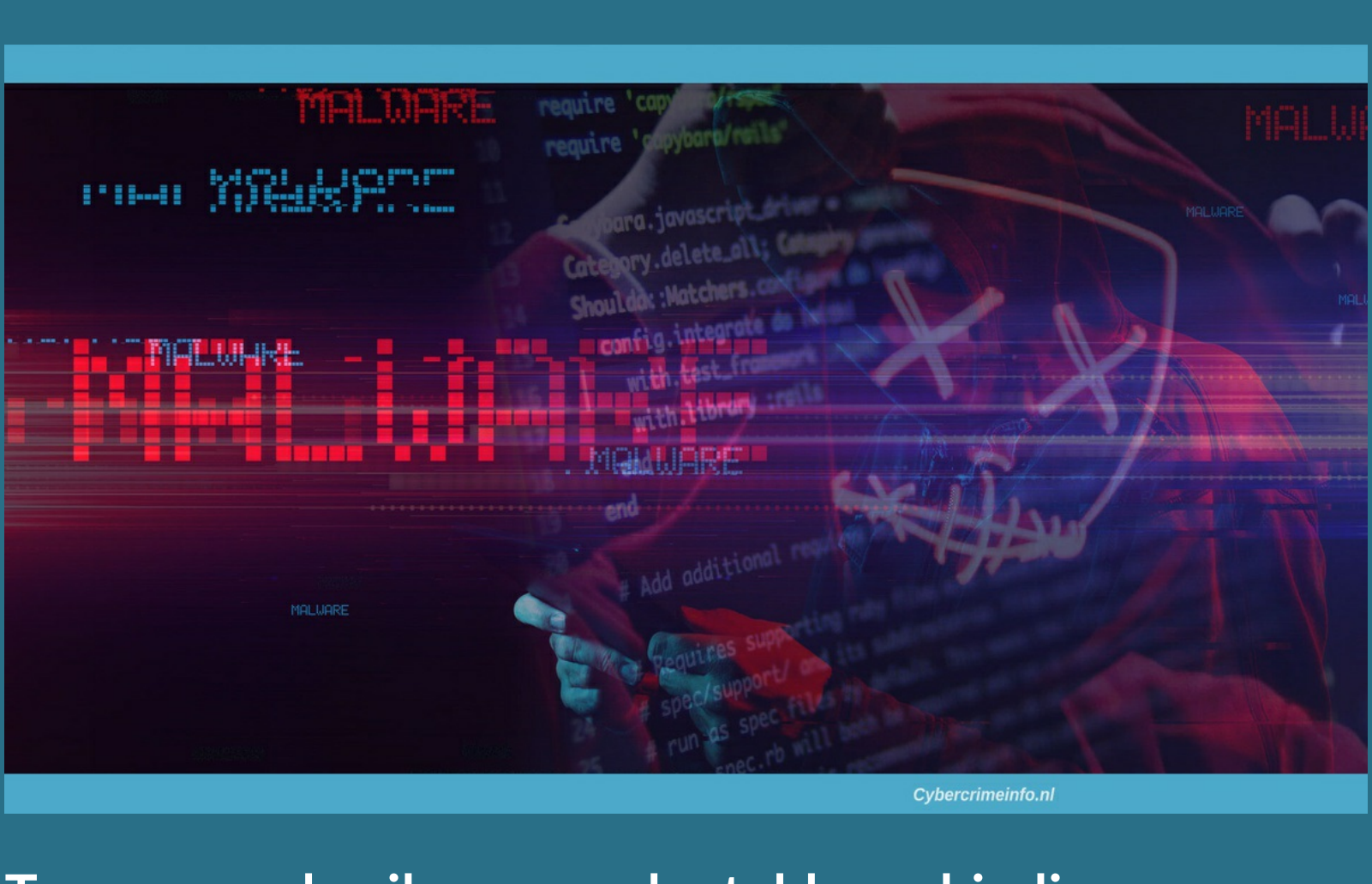
Bekijk de webversie

Nieuwsbrief 194 - Week 04-2022

Ruim 30.000 domeinnaamhouders gewaarschuwd voor malware en phishing

De Stichting Internet Domeinregistratie Nederland (SIDN), de organisatie die de domeinnamen voor het .nl-domein beheert, heeft in een jaar tijd ruim 30.000 domeinnaamhouders gewaarschuwd voor malware en phishing. Dat meldt de organisatie in een transparantierapport (pdf onderaan het artikel). Het gaat om de periode vanaf het vierde kwartaal van 2020 tot en met het derde kwartaal van 2021. Bij de meeste gevallen betrof het waarschuwingen voor phishing.

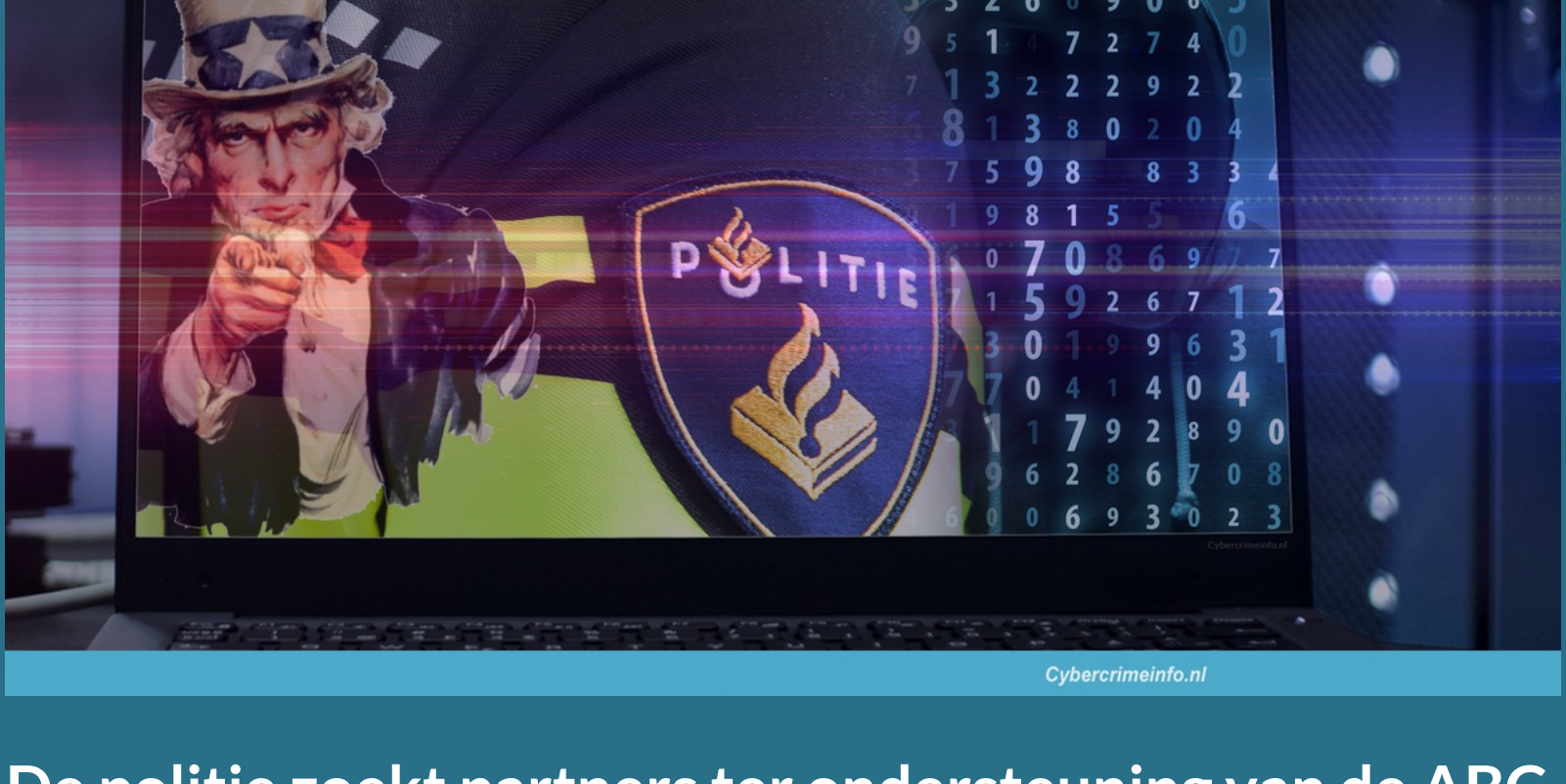
Lees verder



Toename gebruik van versleutelde verbindingen voor het afleveren van zerodays en malware

Het aantal malwarebesmettingen op eindpoints oversteeg in Q3 van 2021 al het totale volume van 2020. Ook het aantal zero-day-aanvallen met malware dat binnenkomt via versleutelde verbindingen is gestegen. Dat concludeert WatchGuard Technologies in de nieuwste editie van het Internet Security Report. Het Internet Security Report informeert organisaties over het actuele dreigingslandschap en draagt best practices voor IT-beveiliging aan.

Lees verder



De politie zoekt partners ter ondersteuning van de ABC campagne

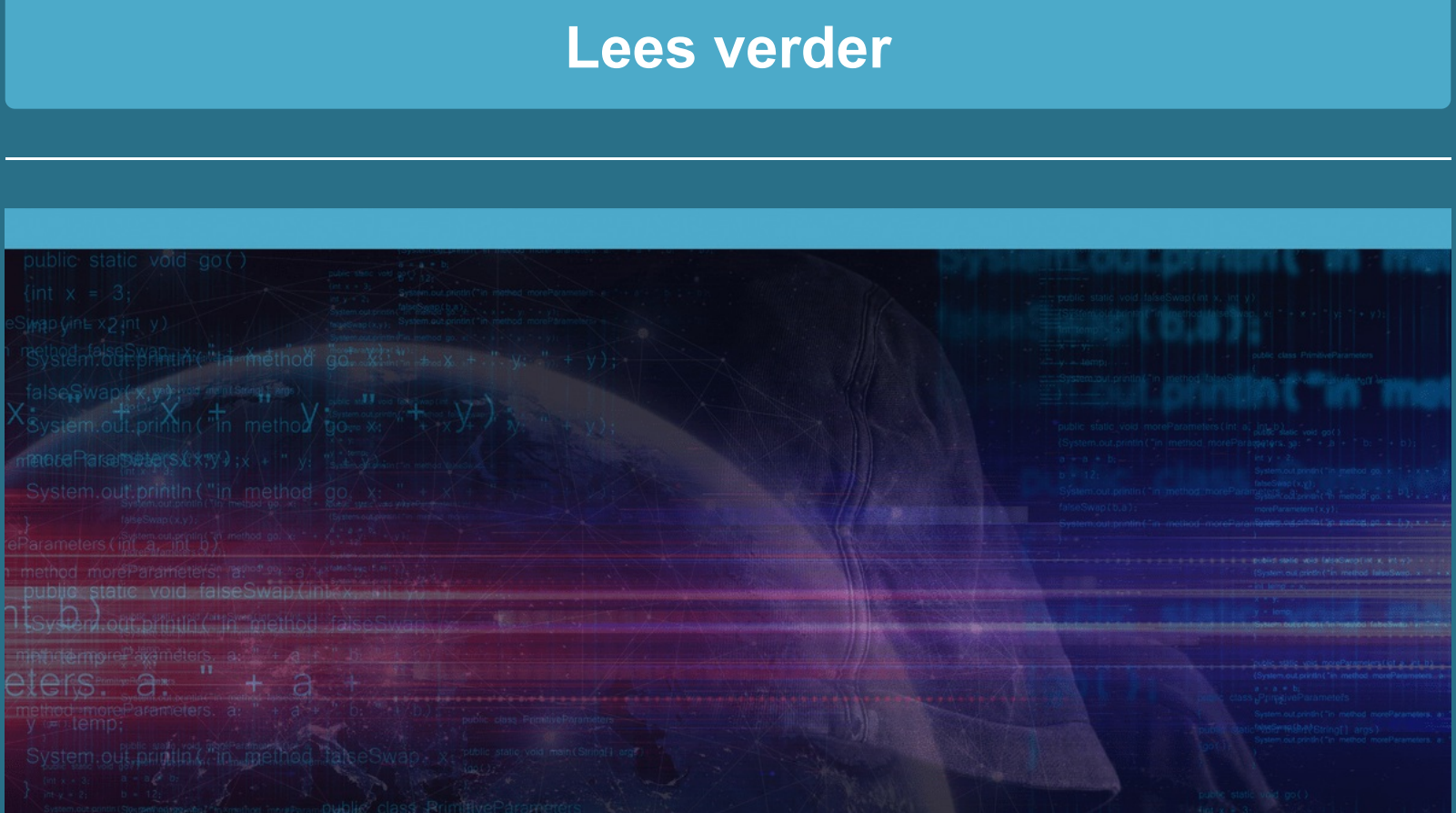
Nog elke dag zien we digitale criminaliteit toenemen. Door verschillende partners worden proactieve, preventieve maar ook repressieve activiteiten ingezet om digitaal slachtofferschap tegen te gaan. Preventie is een belangrijke sleutel om digitale criminaliteit terug te dringen. Anders dan bij klassieke criminaliteit, maken cybercriminelen gebruik van gelegenheden die zich voordoen en die onbedoeld door het slachtoffer wordt geboden.

Lees verder

Oorlog in cyberspace in volle gang omtrent situatie Rusland-Oekraïne

Bedrijven, organisaties en veiligheidsexperts zijn bezorgd over de gespannen situatie die momenteel heerst tussen Oekraïne en Rusland. In het verleden hebben spanningen tussen deze landen geleid tot digitale aanvallen in Nederland. Het is niet uit te sluiten dat we in de nabije toekomst hier opnieuw mee geconfronteerd worden.

Lees verder



Cyberaanvallen: 'Een crisismanager moet inhoudelijk snappen waar het over gaat'

De kans dat een organisatie getroffen wordt door een cyberincident is 1 op 8. Maar het voorbereiden op en het oefenen van een cybercrisis wordt nauwelijks gedaan. "Het beperken van de schade zit in een goede voorbereiding", stelt Job Kuijpers, CEO bij EYE Security. Organisaties ontdekken een cyberincident vaak te laat. Op dat moment is er al iets aan de hand; er is veel geld verdwenen, data gestolen of alle systemen zijn op slot gezet door ransomware. Dat is het moment dat de processen stil komen te liggen en dat het duidelijk wordt dat een organisatie getroffen is.

Lees verder

Ruim helft van de jongeren die ICT-onderwijs volgen plegen cyberdelicten

Een groot deel van de Nederlandse jongeren die ICT-onderwijs volgen, maakt zich wel eens schuldig aan cybercrime. Dit blijkt uit onderzoek van de VU en het NSCR. Toch blijkt het niet zo makkelijk om onderscheid te maken tussen jongeren die ´goede´ en ´slechte´ dingen doen met computers en ICT. Veel jongeren die online de wet overtreden, gebruiken hun ICT-vaardigheden tegelijkertijd om anderen te helpen of zich maatschappelijk in te zetten. Dit betekent dat jonge daders van online delicten kunnen worden gestimuleerd om hun vaardigheden positief in te zetten.

Lees verder

Pretexting: Het belangrijkste aspect van pretexting is het vertrouwen winnen

Internetoplichters zoeken steeds weer nieuwe manieren om nietsvermoedende consumenten geld afhandig te maken. Zo nemen criminelen een valse identiteit aan door middel van spoofing of doen ze zich voor als een familielid via WhatsApp-fraude. Nu is er iets nieuws: pretexting. In dit artikel leggen we uit wat het is en wat je ertegen kunt doen.

Lees verder

Overzicht cyberaanvallen week 03-2022

FBI verdenkt Trickbot groep van ontwikkeling Diavol ransomware, account gegevens buitgemaakt bij ransomware aanval OpenSubtitles.org en nieuwe White Rabbit ransomware gekoppeld aan FIN8 hacking groep. Hier het overzicht van afgelopen week en het nieuws van dag tot dag.

Bekijk het weekoverzicht

Phishing, nepshop en fraude meldingen week 04-2022

Het melden van 'digitale oplichting' pogingen is belangrijk, door het melden kunnen we andere potentiële slachtoffers behoeden voor het te laat is. Heb je een phishing mail, smishing bericht of werd je gebeld en vertrouw je het niet? Laat het ons, of onze collega's van Opgelicht?!, Radar, Kassa, of Fraudehelpdesk dan weten, want Samen bestrijden we cybercrime / digitale fraude. Liever anoniem? Klik dan hier. Ben je slachtoffer geworden van oplichting doe dan 'altijd' aangifte bij de politie.

Bekijk het weekoverzicht

Datalek nieuws en overzicht week 04-2022

Een datalek kan ernstige gevolgen hebben, soms worden levens totaal verwoest door dat er identiteit fraude mee gepleegd wordt. Heb je een vermoeden van een datalek en is het nog niet gemeld of weet je niet als het gemeld is aan de 'Autoriteit persoons gegevens (AP)' laat het ons dan weten, want bij een datalek moet er snel gehandeld worden om mogelijke catastrofale gevolgen te voorkomen.

Bekijk het weekoverzicht

Amsterdam - Phishing via advertentie keukenapparaat

Wie herkent deze personen?

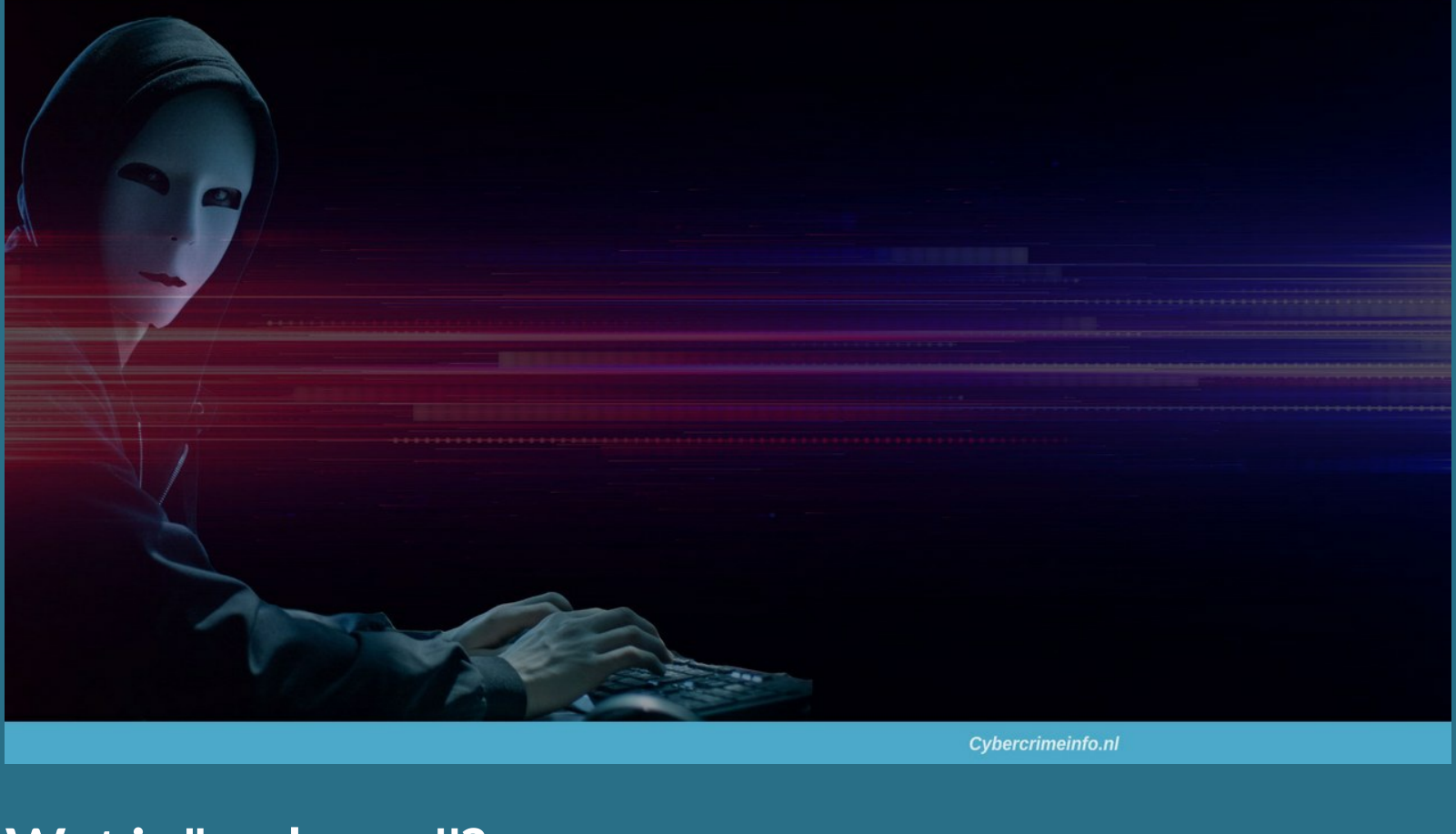
Donderdagavond 5 augustus 2021 heeft een nog onbekende man bij een elektronicawinkel aan de Johan Cruijff Boulevard in Amsterdam-Zuidoost betaald met een frauduleus verkregen betaalmiddel. De betaalgegevens werden twee dagen eerder na een zogenaamde verkoop via een social media platform verkregen.

Lees verder

8 jaar gevangenis en 8,4 miljoen dollar terug betalen voor beheerder van DeepDotWeb

Een 37-jarige Israëlische man die de website DeepDotWeb beheerde is in de Verenigde Staten veroordeeld tot een gevangenisstraf van acht jaar en een maand. Daarnaast doet hij afstand van 8,4 miljoen dollar die hij via de website verdiende. Dat laat het Amerikaanse ministerie van Justitie weten.

Lees verder



Wat is "malware"?

Hoe goed ben jij inmiddels op de hoogte van cybercrime begrippen en vormen?

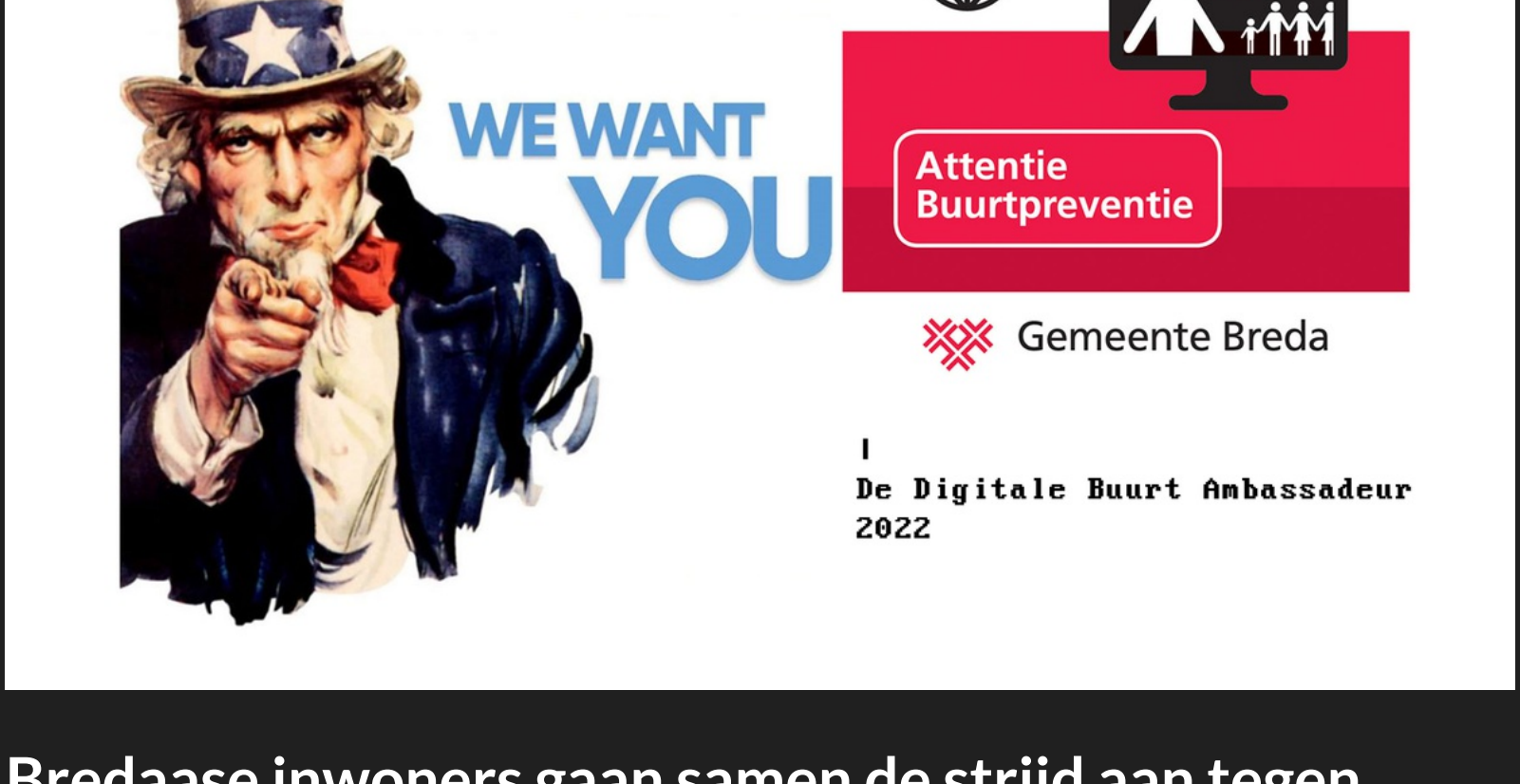
Weet jij wat 'malware' is?
Nee, geen nood, hier kun je het lezen.

Wil je meer vormen en begrippen leren kennen?

Vernieuwde pagina 'Van A tot Z' (nu nog overzichtelijker)

Van A tot Z

Share Tweet Share Pinterest



Bredaase inwoners gaan samen de strijd aan tegen cybercrime

Over cybercrime weten we nog niet zo veel en als we dan slachtoffers hiervan worden is er vaak sprake van schaamte. Bij vragen of behoefte aan ondersteuning weten bewoners vaak niet waar ze terecht kunnen. Daarom hebben wij sinds 2019 in Breda het project 'cyber ambassadeurs' om bewoners meer te betrekken bij digitale veiligheid.

Lees verder

Wekelijks programma Cybercrimeinfo

Dagelijks nieuwe artikelen op Cybercrimeinfo, een overzicht van de actuele aanvallen en wekelijks terugkerende onderwerpen, hier het programma:

- Ma: Cyberaanvallen / ransomware weekoverzicht
- Di: Gezochte persoon cybercrime / digitale fraude
- Za: Darkweb gerelateerd bericht
- Zo: Oplichting en datalekken weekoverzicht
- Op zondagavond om 19:00 wordt de wekelijkse nieuwsbrief verstuurd.

Lees verder

CYBERCRIMEINFO.NL

Mag ik foto's of plaatjes die ik op Cybercrimeinfo vind gebruiken voor mijn site of blog?

Mag ik foto's of plaatjes die ik op Cybercrimeinfo vind gebruiken voor mijn site of blog? Het korte antwoord is Ja.
Maar hoe zit dit eigenlijk met rechten en het gebruiken van foto's die je op Internet vindt?

Lees verder

Steun Cybercrimeinfo zodat we kunnen blijven bestaan

Om deze website te runnen en iedereen te kunnen blijven voorzien van het laatste nieuws, tips en tricks over digitale criminaliteit, zijn wij op zoek naar donateurs. Hiervan kunnen we onder andere nieuwe apparatuur aanschaffen, want deze hele site draait op vrijwilligers. Kortom, wij kunnen niet zonder jouw steun! Help je mee in de strijd tegen cybercrime?
Iedere donatie, hoe klein ook, is van harte welkom. Alvast bedankt namens het hele team van Cybercrimeinfo.

Doneren kan al vanaf 5 euro!

Doneer