Nieuwsbrief 275 - Week 33-2023

Uw scherm verbergt geheimen: De cyberaanvallen waar je vanaf moet weten

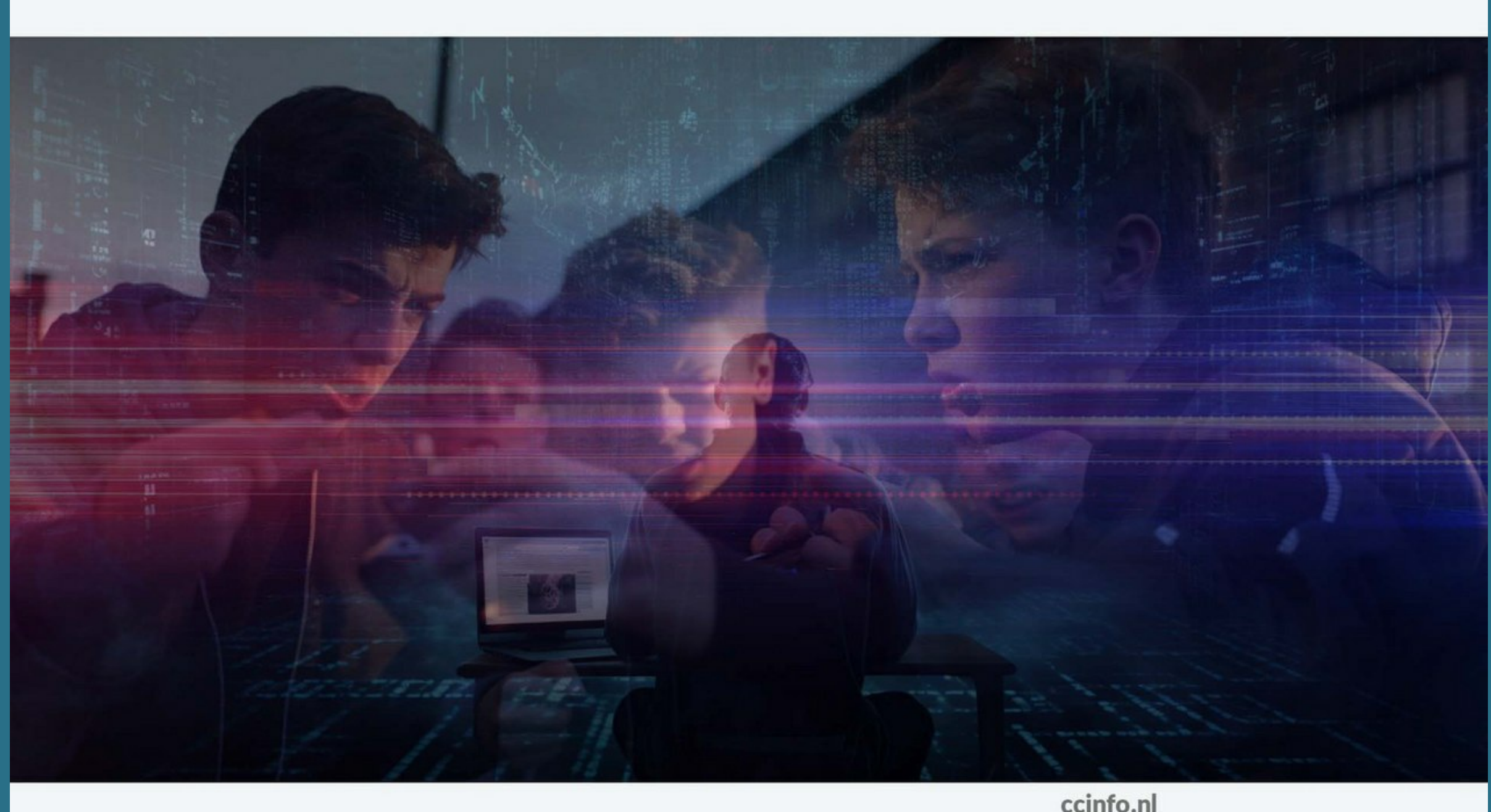
In de moderne digitale wereld is het gemakkelijk om te vergeten dat elk apparaat, elke klik, en elke download potentiële gevaren met zich meebrengt. Terwijl technologie ons leven op vele manieren heeft verbeterd, heeft het ook de deur geopend voor een reeks cyberdreigingen die zowel individuen als bedrijven kunnen treffen. In dit artikel duiken we diep in de meest voorkomende cyberaanvallen en bieden we inzicht in hoe je jezelf kunt beschermen. Van virussen tot SQL-injecties, blijf veilig in de digitale wereld met CyberCrimeInfo.nl, de bibliotheek voor de bestrijding van digitale criminaliteit.

Lees verder

De dunne lijn tussen cybercriminaliteit en ethisch hacken: de 15 soorten hackers die je moet kennen

In de digitale wereld van vandaag groeit het belang van cybersecurity, aangezien het aantal met internet verbonden apparaten toeneemt. Hackers zijn divers in 2023. Black Hat hackers richten zich op activiteiten zoals creditcardgegevens stelen en ransomware-aanvallen. White Hat hackers testen systemen ethisch. Gray Hat hackers, in een moreel grijs gebied, onthullen soms kwetsbaarheden voor een beloning. Blue Hat hackers identificeren softwarefouten vóór de lancering. Red Hat hackers vallen Black Hats aan. Elite hackers voeren geavanceerde aanvallen uit. Green Hat hackers zijn nieuwsgierig en kunnen White Hats worden. Script kiddies zijn onervaren. Hacktivists beïnvloeden politiek en bedrijven. Gesponsorde hackers werken voor overheden. Cyberterroristen zaaien angst en schade. Gaming hackers richten zich op gamers. Cryptojackers delven cryptocurrency met geïnfecteerde apparaten. Het begrijpen van deze diversiteit is cruciaal voor cybersecurity.

Lees verder



Het Darkweb en de verontrustende trend van 'Happy Slapping'

In een tijd waarin technologie en sociale media diep verweven zijn met het leven van jongeren, rijst een verontrustend fenomeen op: "happy slapping". Hierbij wordt geweld gefilmd en gedeeld voor amusement en aanzien, met diepe wortels in de digitale cultuur en het darkweb. "Happy slapping" betekent doelbewust het vernederen en slaan van iemand filmen, om de video online te delen voor erkenning. Wat nog zorgwekkender is, is de link tussen "happy slapping" en het darkweb, waar sommige sites alleen toegankelijk zijn na het maken van gewelddadige video's. Voor slachtoffers is de impact tweeledig, met blijvende online vernedering. Daders en delers riskeren juridische consequenties, en mediawijsheid is cruciaal om dit te bestrijden. Nederland heeft ook incidenten gezien, en de wetgeving pakt online geweld aan met boetes tot gevangenisstraffen. Scholen en gemeenschappen werken aan bewustwording om een veiligere online omgeving te bevorderen.

Lees verder

Tip van de week: Cybercriminelen in je computer? Deel 4: Het reinigen en beschermen van Apple-apparaten

Bescherming en reiniging van Apple-apparaten tegen cyberaanvallen zijn van vitaal belang. Hoewel Apple-apparaten bekendstaan om hun sterke beveiliging, zijn ze niet onkwetsbaar. Dit artikel bespreekt effectieve stappen om geïnfecteerde apparaten te identificeren en reinigen. Symptomen zoals vertragingen, onverwachte pop-ups, en batterijafname kunnen tekenen van infectie zijn. Het is essentieel om geïnfecteerde apparaten te isoleren en ze te scannen met antivirussoftware. Het opstarten in de veilige modus kan helpen problemen te diagnosticeren. Inlogonderdelen kunnen worden verwijderd als het probleem niet in de veilige modus optreedt. In ernstige gevallen kan systeemherstel nodig zijn, maar zorg voor een back-up van belangrijke bestanden. Houd altijd je besturingssysteem en apps up-to-date en open alleen vertrouwde software op je Mac. Volg deze stappen om je Apple-apparaat te beschermen en schoon te houden.

Lees verder

Overzicht cyberaanvallen week 32-2023

In week 32 van 2023 werd de digitale wereld opnieuw opgeschrikt door verontrustende cyberaanvallen. Van de Rhysida Ransomware, gericht op de gezondheidszorg, tot de Lapsus$ Hackers die hun dreiging vergroten met geavanceerde SIM-swapping aanvallen. Zelfs oude beveiligingslekken blijven niet gespaard, zoals blijkt uit de Gafgyt Malware-aanval op Zyxel Routers. Nederland ontkwam niet aan deze digitale dreigingen, met aanvallen op de Kamer van Koophandel, de website van Gemeente Vlaardingen, diverse banken, en zelfs het Maastricht Aachen Airport en OV-NL werden getroffen. Bovendien zijn er nieuwe bedreigingen ontdekt, gericht op specifieke technologieën en platforms, waaronder VPN-gebruikers op iOS en macOS, Microsoft 365-gebruikers en zelfs de AMD Zen-CPU's. Dit artikel biedt een gedetailleerd overzicht van alle cyberaanvallen van de afgelopen week. Lees verder op onze website voor meer informatie.

Bekijk het weekoverzicht

Nootdorp - Bankhelpdesk fraude

Op 17 november 2022 werd een 87-jarige vrouw uit Nootdorp het slachtoffer van een geraffineerde vorm van oplichting, bekend als bankhelpdeskfraude. Een onbekende, die zich voordeed als medewerker van de bank, benaderde de vrouw met het verhaal dat er problemen waren met haar bankrekening. Onder dit voorwendsel wist de nep-medewerker de bankpas van de vrouw in handen te krijgen. Niet veel later werd met deze bankpas geld opgenomen op de Markt in Nootdorp. Daarnaast kocht een onbekende man VVV-bonnen met de gestolen pinpas in het winkelcentrum Parade te Nootdorp. De politie is dringend op zoek naar informatie die kan leiden tot de aanhouding van de verdachte. Voor meer informatie en om het hele artikel te lezen, kunt u terecht op de website van CyberCrimeInfo.nl. Wees altijd alert op dergelijke vormen van fraude en deel nooit persoonlijke bankgegevens met onbekenden, hoe overtuigend hun verhaal ook mag klinken.

Lees verder

AI chatbot assistent Cybercrime en Cybersecurity

"De AI chatbot assistent: elke dag getraind, elke dag sterker in de strijd tegen criminaliteit."

In het huidige digitale tijdperk, waarin cybercriminaliteit steeds vaker voorkomt, is toegang tot betrouwbare informatie en ondersteuning van cruciaal belang. De Cybercrimeinfo AI chatbot staat te allen tijde voor u klaar om uw vragen over cybercriminaliteit, het darkweb en cybersecurity te beantwoorden. Deze chatbot is direct verbonden met de Cybercrimeinfo-database en haalt geen informatie van het internet. De informatie die de bot verschaft, is uitvoerig gecontroleerd en is volledig betrouwbaar.
Wat deze chatbot onderscheidt, zijn de wekelijkse updates over cyberaanvallen, kwetsbaarheden, opsporingsberichten en betrouwbare artikelen aangaande cybersecurity, cybercriminaliteit en het darkweb. Zo hebt u altijd en overal toegang tot een actuele en betrouwbare cyberassistent die 24/7 beschikbaar is

PS: Wist u dat we ook een 'AI chatbot assistent voor Strafrecht en Strafvordering - Hulpofficier en Opsporingsambtenaar' hebben? Gezien de voortdurende ontwikkelingen in de criminaliteit, is het van essentieel belang om up-to-date te blijven met moderne technologieën die efficiënte, snelle en nauwkeurige oplossingen bieden. De AI Chatbot voor Strafrecht en Strafvordering is ontworpen om uitgebreide informatie te bieden over strafrecht en strafvordering. Of u nu opsporingsambtenaar of hulpofficier bent, deze chatbot staat altijd voor u klaar.

AI Chatbot

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

Share Tweet Share Pinterest