



Nieuwsbrief 278 - Week 36-2023



ccinfo.nl

De donkere kant van Telegram: Een onderzoek naar wraakporno en exposing in Nederland

In het digitale tijdperk zijn apps als Telegram onmisbaar geworden voor onze dagelijkse communicatie. Toch schuilt er een donkere kant achter dit soort platforms. Een diepgaand onderzoek onthult een alarmerende trend in Nederlandse Telegram-groepen waar wraakporno en 'exposing' aan de orde van de dag zijn. Niet alleen is dit een ernstige inbreuk op de privacy, maar het heeft ook verstrekkende juridische en psychologische gevolgen. Het gebrek aan actie vanuit Telegram zelf en de uitdagingen voor wetshandhavers maken een gecoördineerde aanpak noodzakelijk. In dit artikel verkennen we de omvang van het probleem, gebaseerd op onderzoek en rapportages, en onderzoeken we waarom een gecoördineerde aanpak essentieel is voor een veiligere digitale omgeving.

[Lees verder](#)



ccinfo.nl

Juice Jacking ontmaskerd: Alles wat je moet weten om je smartphone veilig te houden

Juice jacking is een toenemend risico in de digitale wereld waarin we leven. Deze vorm van cyberaanval richt zich op het compromitteren van smartphones en andere draagbare apparaten door misbruik te maken van openbare USB-oplaadstations. Aanvallers installeren kwaadaardige software op deze stations, waardoor ze toegang krijgen tot aangesloten apparaten en potentieel gevoelige gegevens kunnen stelen. De risico's variëren van diefstal van contactinformatie tot het volledige overnemen van het apparaat, inclusief identiteitsdiefstal en spionage via de camera. Bescherming tegen juice jacking begint met basale stappen zoals het gebruik van je eigen opladers en kabels, en het installeren van betrouwbare beveiligingssoftware op je smartphone. Ook het up-to-date houden van je apparaat en het gebruik van USB-data blockers kunnen helpen om deze dreiging te minimaliseren. Voor meer diepgaande informatie en adviezen, lees het volledige artikel op onze website.

[Lees verder](#)



ccinfo.nl

Analyse van de Genesis Market zaak en de geëiste straf

Het Openbaar Ministerie (OM) in Nederland heeft onlangs een significante straf geëist in de Genesis Market-zaak, waarmee het belang van deze zaak in de strijd tegen cybercriminaliteit wordt onderstreept. De verdachte, een 34-jarige man uit Boskoop, wordt beschuldigd van het illegaal verkrijgen en gebruiken van inloggegevens via deze digitale marktplaats. De OM eist 40 maanden gevangenisstraf tegen de man, die naar verluidt meer dan vijfduizend dollar heeft uitgegeven aan 'botjes', digitale sleutels voor het compromitteren van de accounts van uitwendende slachtoffers. De zaak brengt niet alleen technologische en juridische uitdagingen aan het licht, maar legt ook een immense psychologische last op de slachtoffers. Lees het volledige artikel voor een gedetailleerde analyse van deze zaak en de bredere implicaties voor de cyberbeveiliging.

[Lees verder](#)



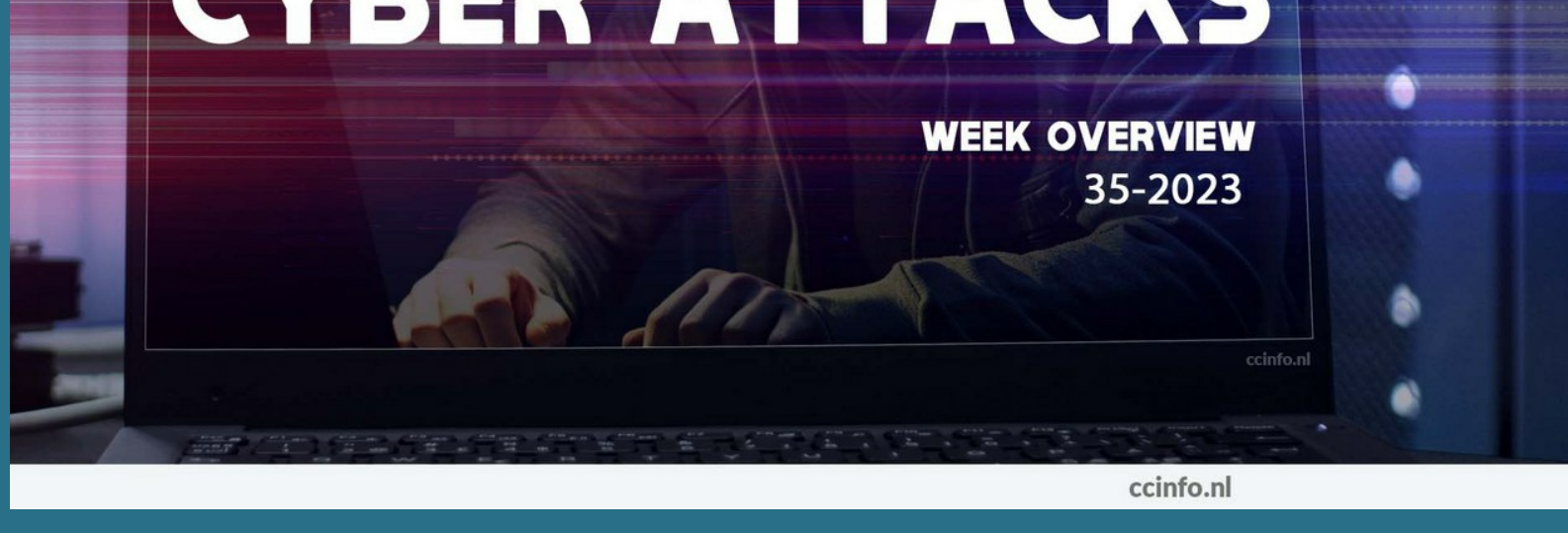
ccinfo.nl

Tip of the week:
Why you should regularly switch off your smartphone

Tip van de Week: Waarom je je smartphone regelmatig moet uitschakelen

Uiteraard is uw smartphone een onmisbaar onderdeel van uw dagelijks leven, maar deze constante beschikbaarheid maakt het ook een ideaal doelwit voor cybercriminelen. Een veelal onderschatte, maar zeer effectieve maatregel voor het verhogen van uw cyberveiligheid is het regelmatig uitschakelen van uw smartphone. Dit simpele gebaar kan namelijk bestaande malwareprocessen onderbreken en tijdelijke data wissen die anders misbruikt zouden kunnen worden. Overheidsinstanties zoals de Amerikaanse NSA adviseren zelfs om dit wekelijks te doen. Het is een kleine actie die een groot verschil kan maken in uw algehele strategie voor cyberveiligheid. Maak er een gewoonte van; uw digitale welzijn zal u dankbaar zijn.

[Lees verder](#)



ccinfo.nl

Overzicht cyberaanvallen week 35-2023

In de 35e week van 2023 is de cybercriminele activiteit wederom toegenomen, waarbij diverse sectoren het doelwit zijn geworden van aandalen. Een bijzonder zorgwekkende ontwikkeling is de ransomware-aanval op het Nederlandse bedrijf Kendrion en het internationale autobedrijf Renault. Sextortion scams, waarbij slachtoffers worden gechanteerd met persoonlijke en vaak gevoelige informatie, zijn ook in opkomst. Verder is er een verhoogd aantal aanvallen geconstateerd op Citrix NetScaler systemen, waarbij geavanceerde methoden worden toegepast om beveiligingsmaatregelen te omzeilen. Het blijft essentieel om up-to-date detectiesystemen te omzeilen. Het blijft essentieel om up-to-date beveiligingsmaatregelen te nemen en bewust te zijn van de nieuwste aanvalstechnieken om deze dreigingen het hoofd te bieden. Voor diepgaande analyses en aanbevelingen voor een betere cyberbeveiliging kunt u verder lezen op onze website.

[Lees verder](#)



ccinfo.nl

Tilburg - Bankhelpdesk fraude

In Tilburg is een ernstig geval van bankhelpdesk fraude gemeld, waarbij gebruik is gemaakt van spoofing. Een man heeft duizenden euro's opgenomen met een gestolen bankpas na zich telefonisch aan te melden als een bankmedewerker. Het slachtoffer werd misleid met een overtuigend verhaal over een virus op haar iPad, waarna haar bankpassen werden opgehaald voor 'onderzoek'. Niet veel later werd er een groot bedrag gepind. De politie is nu op zoek naar de dader en roept het publiek op om tips door te geven via verschillende kanalen.

[Lees verder](#)



AI chatbot assistent Cybercrime en Cybersecurity

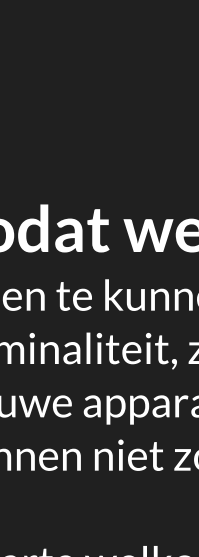
"De AI chatbot assistent: elke dag getraind, elke dag sterker in de strijd tegen criminaliteit."

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 cyberassistente 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](#)



Steen 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 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

Deze e-mail is verzonden aan [\(email\)](#). • Als u geen nieuwsbrief meer wilt ontvangen, kunt u zich [hier afmelden](#). • U kunt ook uw [gegevens inzien en wijzigen](#). • Voor een goede ontvangst voegt u info@cybercrimeinfo.nl toe aan uw adresboek.

