Cybercrimeinfo.nl (ccinfo.nl) Bekijk de webversie

Nieuwsbrief 337

Reading in □□ or another language

Ransomware in Nederland: Groeiende bedreiging voor organisaties en privacy

Ransomware vormt in Nederland een toenemende dreiging voor bedrijven en burgers, met een sterke stijging in aanvallen in 2023. Gebrekkige basisbeveiliging bij organisaties, zoals het ontbreken van meerfactorauthenticatie en trage software-updates, maakt hen kwetsbaar. Een trend die hierbij opvalt, is 'dubbele afpersing': cybercriminelen dreigen met openbaarmaking van gestolen data naast het vergrendelen ervan. De Autoriteit Persoonsgegevens (AP) speelt een belangrijke rol door ransomware-incidenten in kaart te brengen via de meldplicht voor datalekken.

Uit het onderzoek blijkt dat betalen van losgeld geen garantie biedt voor herstel en eerder het criminele verdienmodel versterkt. Slechts een klein aantal bedrijven kiest toch voor betaling, vaak zonder data terug te krijgen. De AP adviseert organisaties om basisbeveiligingsmaatregelen te verbeteren, zoals MFA, sterk wachtwoordbeleid en netwerksegmentatie, om de kans op ransomware-aanvallen te verkleinen en de privacy van hun klanten beter te beschermen.

Lees verder

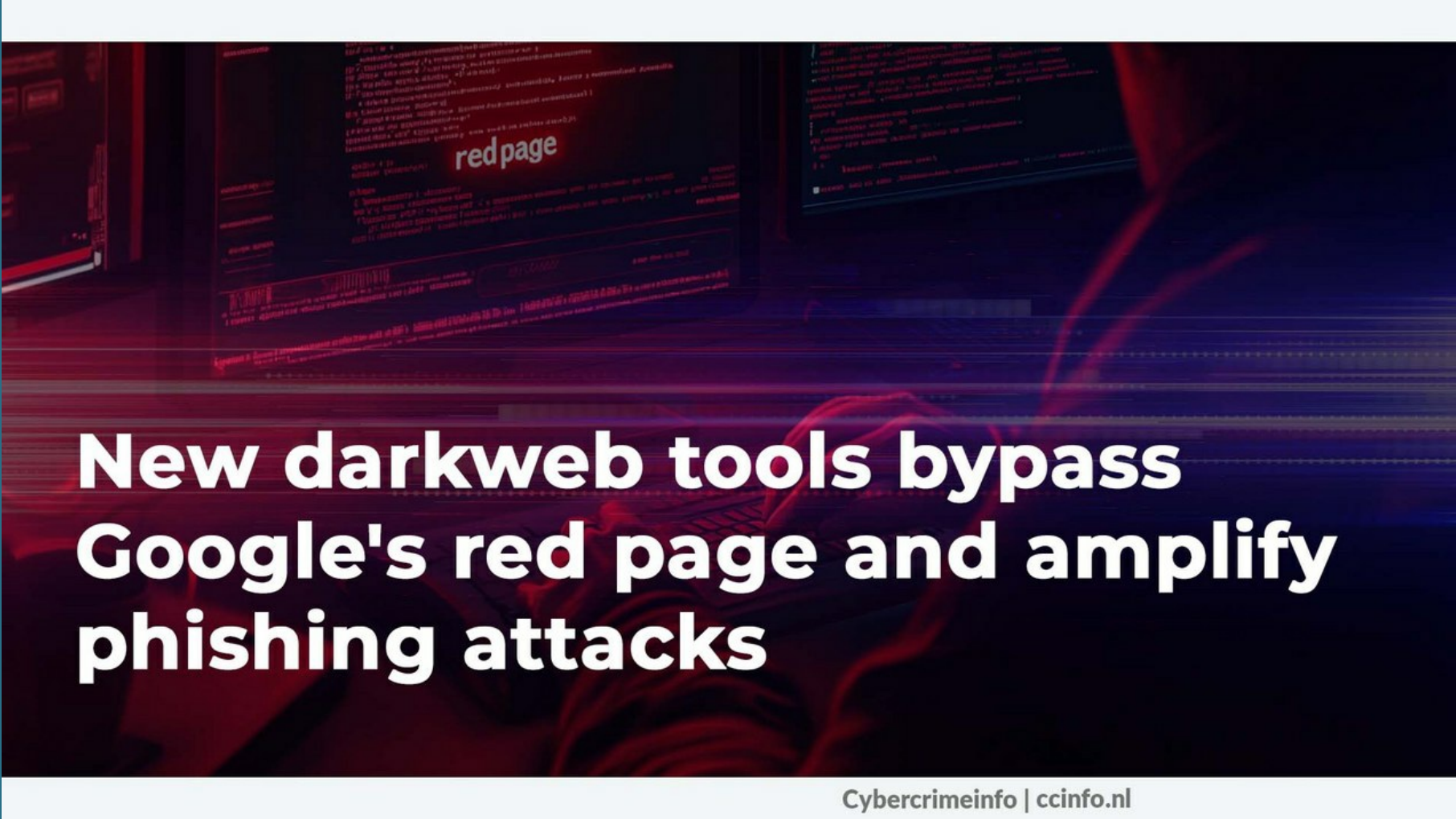
Reading in □□ or another language

Telegram onder druk: bangalijsten verwijderd, maar zorgen blijven

Na stevige druk van Offlimits heeft Telegram recentelijk de zogenoemde "bangalijsten" van zijn platform verwijderd. Deze lijsten bevatten gevoelige gegevens van vrouwen, zoals namen, foto's en contactgegevens, waarbij ze beoordeeld werden op uiterlijk en vermeende seksuele activiteiten. Door de verspreiding van deze lijsten werden veel vrouwen slachtoffer van intimidatie en bedreigingen. Offlimits dwong Telegram tot actie door juridische stappen te ondernemen, gesteund door verschillende organisaties en fondsen, wat resulteerde in een toezegging van Telegram om een speciaal meldkanaal op te richten. Dit meldkanaal stelt Offlimits in staat om toekomstige misstanden sneller te melden.

Hoewel deze lijsten nu uit openbare Telegram-groepen zijn verdwenen, blijft er zorg over gesloten groepen waar schadelijke inhoud nog steeds ongemerkt gedeeld kan worden. De recente acties tegen Telegram worden internationaal ondersteund, en de druk op het platform om verantwoordelijkheid te nemen voor gebruikersveiligheid groeit. Deze ontwikkelingen onderstrepen de noodzaak voor sociale mediaplatformen om proactief op te treden tegen online misbruik.

Lees verder



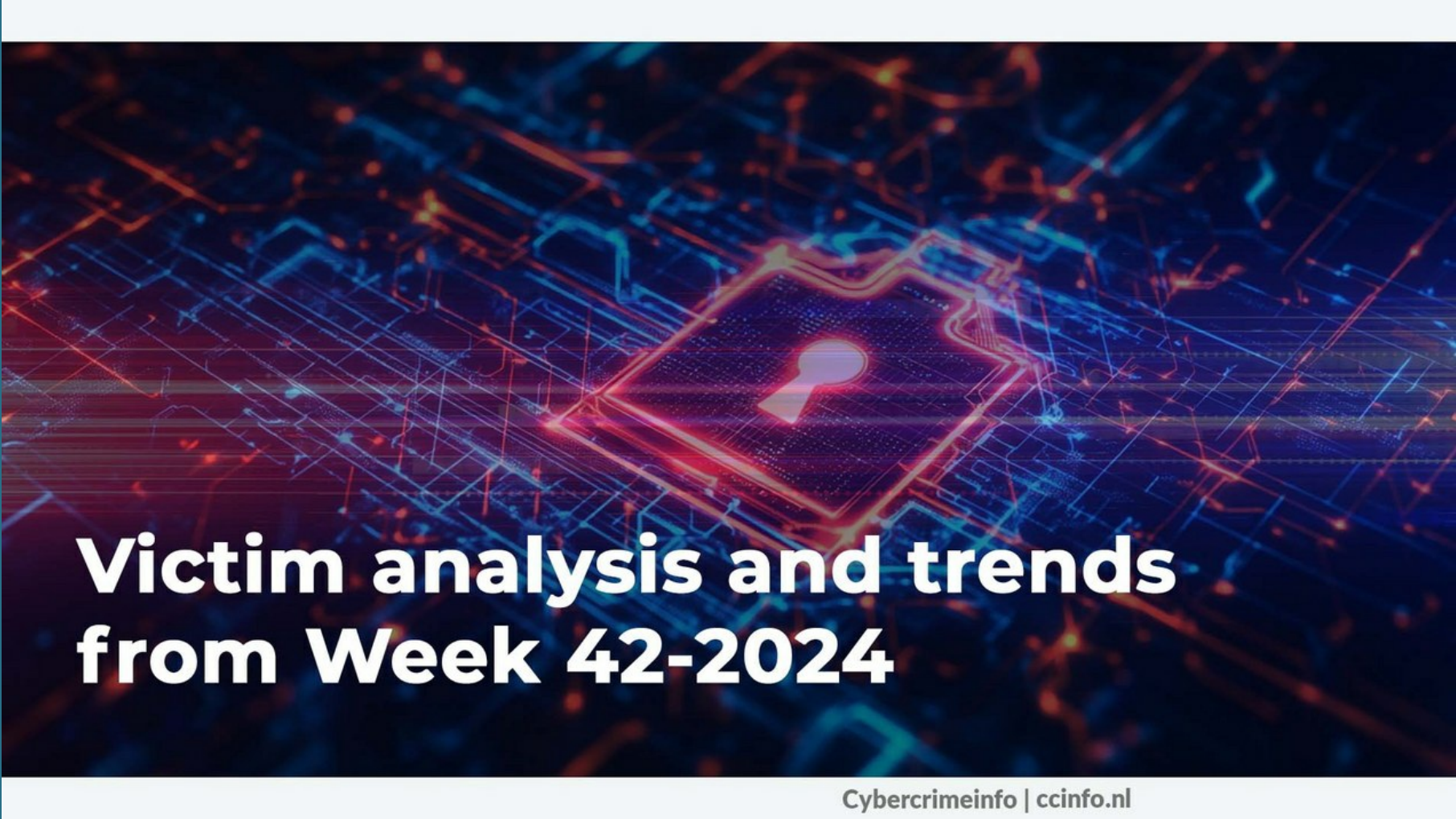
Reading in □□ or another language

Nieuwe darkweb tools omzeilen Google's red page en versterken phishingaanvallen

Recente innovaties op het darkweb stellen cybercriminelen in staat om Google's 'Red Page'-waarschuwing te omzeilen, wat de effectiviteit van phishingaanvallen aanzienlijk verhoogt. Deze nieuwe tools, zoals Otus Anti-Bot en Remove Red, maken gebruik van geavanceerde technologieën zoals IP-filtering, cloaking en geotargeting om beveiligingssystemen te misleiden. Hierdoor blijven malafide websites langer online en moeilijker detecteerbaar voor beveiligingssoftware. Naast deze technologieën speelt ook kunstmatige intelligentie (AI) een groeiende rol in de effectiviteit van anti-bot diensten. AI helpt niet alleen bij het omzeilen van beveiligingsmechanismen maar kan ook patroonherkenning toepassen, waardoor phishingpagina's zich adaptief kunnen aanpassen aan veiligheidsmaatregelen.

De opkomst van Phishing-as-a-Service (PhaaS)-platformen maakt het zelfs voor onervaren criminelen mogelijk om grootschalige phishingcampagnes op te zetten. Om deze bedreigingen tegen te gaan, worden bedrijven aangeraden om geavanceerde beveiligingssystemen te implementeren, e-mailbescherming te versterken en hun personeel op te leiden in cyberveiligheid.

Lees verder



Reading in □□ or another language

Slachtofferanalyse en Trends van Week 42-2024

In week 42 van 2024 zijn wereldwijd bedrijven en organisaties in uiteenlopende sectoren getroffen door ransomware-aanvallen. Cybercriminelen richtten zich vooral op gevoelige data in de gezondheidszorg, overheid en onderwijs, en plaatsten deze vaak op het dark web. Verschillende ransomware-groepen, zoals Play, Medusa, Bianlian, en Blackbasta, vielen bekende bedrijven aan, waaronder een Nederlands voedingsbedrijf en een Amerikaans gezondheidsnetwerk. Ook in de zorgsector veroorzaakten aanvallen verstoringen, zoals bij Boston Children's Health Physicians en DoctorsToYou in de Verenigde Staten.

Niet alleen de private sector, maar ook overheidsinstellingen en scholen werden doelwit van cyberaanvallen. Aanvallen door de Medusa-groep en Rhysida dreigden gegevens van studenten en medewerkers te lekken. Het overzicht laat zien dat cybercriminelen steeds geavanceerder worden en nieuwe aanvalsmethoden toepassen, zoals supply chain-aanvallen en dreigingen van kwantumcomputers, wat de uitdaging voor cybersecurity vergroot. Dit benadrukt de noodzaak voor bedrijven om hun beveiligingsmaatregelen voortdurend te versterken.

Lees verder

Reading in □□ or another language

Telefoonspoofing: Hoe oplichters met bekende bedrijven je vertrouwen winnen

Telefoonspoofing is een oplichtingstechniek waarbij criminelen een vals telefoonnummer gebruiken dat lijkt op dat van een vertrouwd bedrijf, zoals PayPal of Amazon. Door deze vorm van bedrog vertrouwen slachtoffers de oproep sneller en zijn ze geneigd gehoor te geven aan instructies, zoals het delen van persoonlijke informatie of geld overmaken naar een 'veilige rekening'. In oktober registreerde de Fraudehelpdesk meer dan 800 meldingen, wat wijst op een sterke toename van deze oplichting.

Herkenbare signalen van spoofing-oproepen zijn onder andere automatische berichten die om directe actie vragen, een dreigende toon, en verzoeken om gevoelige informatie. Het is belangrijk om bij twijfel op te hangen en zelf het officiële nummer van het betreffende bedrijf te bellen. Deze fraudevorm blijft zich ontwikkelen, wat bewustzijn en alertheid noodzakelijk maakt om schade en identiteitsdiefstal te voorkomen.

Lees verder

Reading in □□ or another language

Dordrecht - Nepagent

In Dordrecht is een oplichter actief die zich voordoet als politieagent. Op 24 februari 2024 misleidde hij een bejaard echtpaar van 87 en 89 jaar oud door aan te bellen en hun pinpassen en sieraden in beslag te nemen. Vervolgens maakte hij €1900 over met de gestolen passen. De man was in burger en haalde de waardevolle spullen persoonlijk bij het echtpaar op. Later die dag werden camerabeelden van hem gemaakt bij een pinautomaat.

De politie roept het publiek op om te helpen bij de identificatie van deze nepagent. Dit soort oplichting, waarbij criminelen zich voordoen als autoriteiten, komt steeds vaker voor. Nepagenten spelen in op het vertrouwen dat mensen in de politie hebben, en proberen zo persoonlijke gegevens en waardevolle spullen te verkrijgen. De politie adviseert om altijd legitimatie te vragen en geen informatie af te staan zonder verificatie.

Lees verder

Reading in □□ or another language

Verbeter je cyberveiligheid: Test je kennis met onze interactieve quizzen

Verken de wereld van cybersecurity en het darkweb met onze interactieve quizzen op CyberCrimeInfo. Of je nu een beginner bent of een doorgewinterde expert, onze quizzen bieden een leuke en uitdagende manier om je kennis uit te breiden.

Wat kun je verwachten?

- **Leer in je eigen tempo:** Ontdek en test je vaardigheden wanneer het jou het beste uitkomt.
- **Ontvang feedback:** Krijg gedetailleerde feedback na elke quiz, zodat je precies weet waar je staat en waar je nog kunt verbeteren.
- **Verdien speciale erkenning:** Behaal een perfecte score en ontvang speciale erkenning voor je prestaties.

Ben je klaar om je kennis te testen en jezelf te meten met anderen? Begin vandaag nog aan je leerreis en vraag je toegangscode aan!

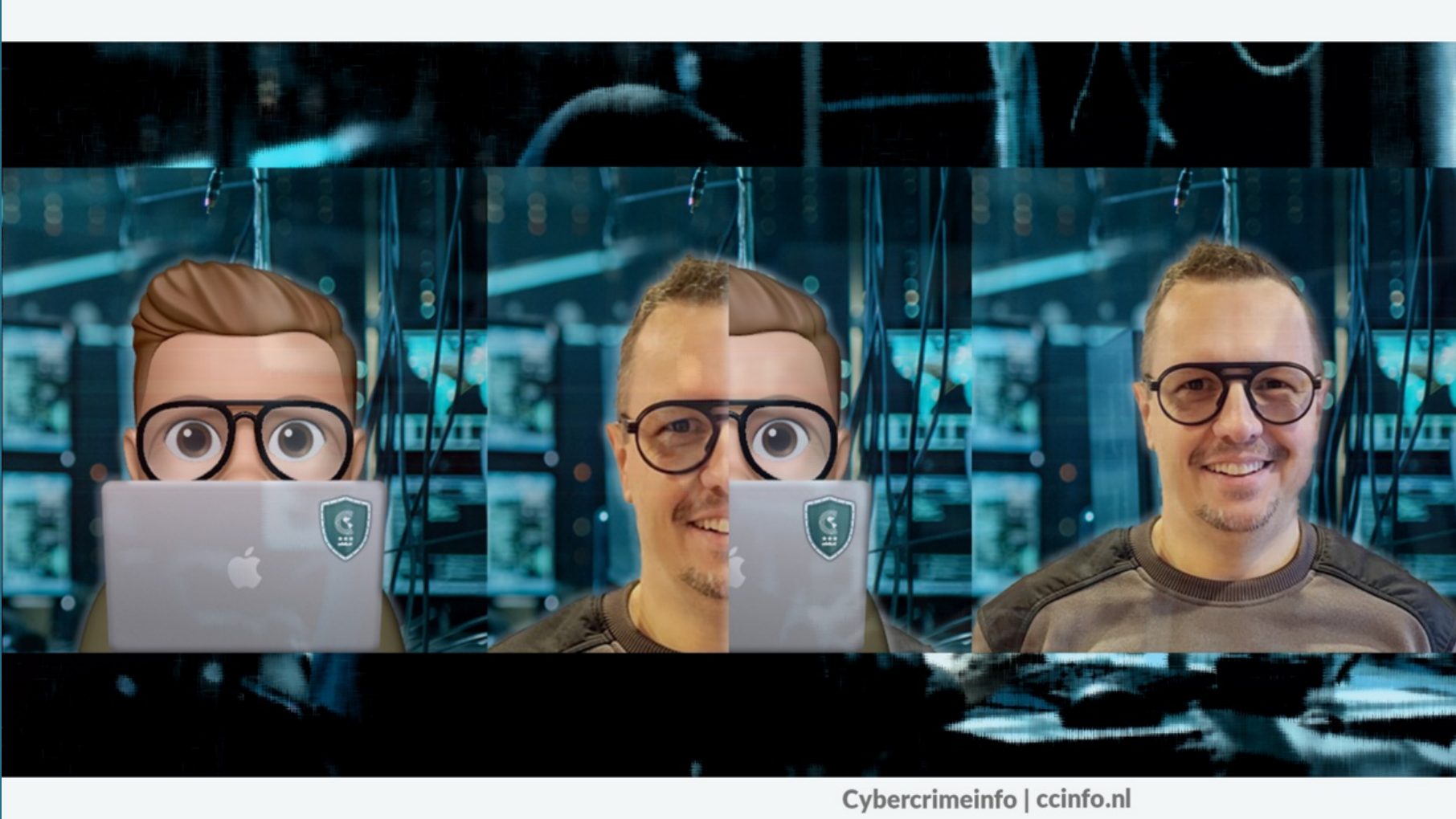
Naar quizzen

De Perfecte Score Club!

Topscorer	Punten	Wanneer
Joost W.	10	04-08-2024
Jasper	10	23-05-2024
Johan	10	16-03-2024
Philip S.	9	17-03-2024
Maxim	9	16-03-2024
Aart	7	21-06-2024
Thijs	7	09-04-2024
Kenan	7	30-03-2024
	NIEUW TOEGEVOEGD	
Lieke F.	4	27-10-2024

Maximaal te behalen **punten: 20**
Aantal deelnemers tot nu toe: 941

Totaal overzicht De Perfecte Score Club!



Reading in □□ or another language

Waarom jouw donatie aan Cybercrimeinfo essentieel is

Beste lezer,
In een wereld waar digitale dreigingen steeds geavanceerder en talrijker worden, speelt Cybercrimeinfo een cruciale rol in de strijd tegen cybercriminaliteit. Wij zijn een onafhankelijke organisatie, gedreven door vrijwilligers, die zich inzet voor het informeren en beschermen van het publiek tegen de gevaren van het digitale tijdperk.
Jouw donatie maakt het verschil. Hier is waarom:

1. **Onafhankelijke en Belangrijke Bron van Informatie:** Cybercrimeinfo is geen onderdeel van de Nederlandse Politie. Wij bieden een onpartijdige en toegankelijke bron van actuele informatie over cyberdreigingen, oplichtingstechnieken en preventiemethoden.
2. **Bijdragen aan Bewustwording en Preventie:** Door te doneren help je ons in de missie om kennis en bewustzijn over cybercriminaliteit te vergroten. Onze artikelen, nieuwsupdates en praktische tips dragen bij aan het voorkomen van digitale misdrijven.
3. **Ondersteuning van Onze Operationele Kosten:** Donaties worden direct gebruikt voor het hosten van de website en het vernieuwen van onze technologische middelen. Dit stelt ons in staat om op de voet te volgen hoe cybercriminelen opereren en jullie te informeren over de nieuwste digitale gevaren.

Elke bijdrage, hoe klein ook, is van onschatbare waarde in onze continue strijd tegen cybercriminaliteit. Met jouw steun kunnen we blijven werken aan een veiliger digitaal landschap voor iedereen.
We waarderen je steun enorm en bedanken je alvast voor je bijdrage aan deze belangrijke zaak.

Doneren kan via de **doneer pagina** (Kies nu zelf het bedrag dat je wilt doneren!) of via onderstaande QR code.

Met vriendelijke groet,
Het team van Cybercrimeinfo

Doneer | Cybercrimeinfo.nl (ccinfo.nl)

Doneer pagina

Geen budget? Geen probleem!

Help ons de zichtbaarheid van Cybercrimeinfo te vergroten met jouw Google review!

Laat jouw stem horen: Steun ons met een Google review!

Wij streven er voortdurend naar om de zichtbaarheid en bereikbaarheid van Cybercrimeinfo te verbeteren. Een fantastische manier waarop jij ons hierbij kunt helpen, is door een review achter te laten op Google. Jouw feedback is onmisbaar voor ons en helpt anderen om ons makkelijker te vinden.
Het plaatsen van een recensie is simpel en kost slechts een minuutje van je tijd. Klik op de volgende link om jouw ervaringen te delen: **Schrijf een review**.
Elke review draagt bij aan onze missie om iedereen beter te informeren over cyberveiligheid. Jouw steun is voor ons ontzettend waardevol! Hartelijk dank voor je betrokkenheid.

Non-profit team Cybercrimeinfo

Share Tweet Share Pinterest