Cybercrimeinfo.nl (ccinfo.nl) Bekijk de webversie

Nieuwsbrief 341

Reading in ▯▯ or another language

De verborgen cyberdreigingen achter populaire koopjesapps

Apps als Temu en TikTok trekken miljoenen gebruikers met scherpe aanbiedingen en verslavende content. Toch schuilt achter dit gemak een groot risico. Temu vraagt bijvoorbeeld toegang tot gevoelige functies op je telefoon, zoals je wifi-netwerk en camera, terwijl TikTok enorme hoeveelheden gebruikersgegevens verzamelt. Deze gegevens kunnen worden misbruikt voor spionage of andere malafide activiteiten, vooral omdat veel van deze apps afkomstig zijn uit landen met actieve cyberprogramma's zoals China en Rusland.

De Nederlandse overheid heeft al stappen ondernomen, zoals het verbieden van apps uit risicolanden op werktelefoons. Maar consumenten blijven kwetsbaar, mede door manipulatieve technieken die impulsaankopen stimuleren en kritische afwegingen bemoeilijken.

Om jezelf te beschermen, is het belangrijk om machtigingen van apps te controleren, een VPN te gebruiken, je apparaat up-to-date te houden en reviews te lezen. Veiligheid begint bij bewustwording en het maken van slimme keuzes, zelfs als dat betekent dat je iets meer betaalt.

Lees verder

Reading in ▯▯ or another language

Online fraude in 2024: Hoe cybercriminelen steeds slimmer te werk gaan

Online fraude blijft een groeiend probleem met steeds geavanceerdere methoden. In 2023 registreerde de politie bijna 70.000 gevallen, maar de werkelijke aantallen liggen veel hoger vanwege onderrapportage. Fraudeurs benutten de digitalisering met vormen als aankoopfraude, phishing en bankhelpdeskfraude. Ze gebruiken social engineering om vertrouwen te winnen en slachtoffers te manipuleren.

Populaire fraudevormen zijn onder meer betaalverzoekfraude via berichtenapps, sextortion met intieme beelden, en beleggingsfraude gericht op financieel stabiele personen. Bovendien opereren georganiseerde groepen met technieken zoals Remote Access Tools en deepfake-technologie, wat nieuwe risico's creëert.

Preventie blijft essentieel: slachtoffers moeten alert zijn op verdachte berichten en veilige betaalmethoden gebruiken. Overheden, bedrijven en individuen moeten samen werken aan betere beveiliging en bewustwording. Door innovatie en samenwerking kan de strijd tegen online fraude worden opgevoerd.

Lees verder

Reading in ▯▯ or another language

De Russische digitale drugsmarkt: Hoe technologie de onderwereld beheerst

De Russische illegale drugsmarkt heeft een transformatie doorgemaakt door het gebruik van geavanceerde technologieën zoals anonieme platforms, cryptocurrencies en innovatieve logistieke systemen zoals Dead Drops. Dead Drops maakt het mogelijk om drugs op geheime locaties achter te laten, waarvan kopers via GPS-coördinaten de exacte plek te weten komen, zonder direct contact met dealers.

Online platforms functioneren als professionele e-commerce websites en gebruiken slimme marketingtechnieken, zoals gamification en loyaliteitsprogramma's, om hun klantenbestand uit te breiden. Cryptocurrencies, vooral Monero, bieden anonieme betalingsmogelijkheden, wat opsporing door autoriteiten bemoeilijkt.

Met een jaarlijkse omzet van $1,5 miljard in 2023 groeit deze industrie internationaal, wat handhaving en wetgeving voor enorme uitdagingen stelt. Internationale samenwerking, technologische innovatie en striktere regelgeving zijn essentieel om deze groeiende dreiging het hoofd te bieden.

Lees verder

Reading in ▯▯ or another language

Slachtofferanalyse en Trends van Week 45-2024

In week 46 van 2024 waren wereldwijd talloze cyberaanvallen en datalekken. In Nederland en België werden onder meer Potteau.be, Klarenbeek Transport en de Rhedens School getroffen door ransomware, met aanzienlijke verstoringen en risico's voor gevoelige gegevens. Ook de Israëlische ambassade in Den Haag werd doelwit van een hackersgroep.

Globaal domineerden ransomwaregroepen zoals Hunters en Blacksuit, met aanvallen op diverse sectoren, van gezondheidszorg tot logistiek. Nieuwe malware zoals Fickle Stealer en SpyNote toonden de toenemende geavanceerdheid van cyberdreigingen. Daarnaast zorgden massale datalekken, waaronder miljoenen Instagram- en Roblox-accounts, voor ernstige privacyschendingen.

Deze incidenten benadrukken de noodzaak van proactieve maatregelen, zoals tweefactorauthenticatie, beveiligingsaudits en bewustwordingstrainingen. Organisaties moeten zich blijven aanpassen aan de snel evoluerende dreigingen om digitale weerbaarheid te vergroten en schade te beperken.

Lees verder

Reading in ▯▯ or another language

Noord-Korea's cyberstrategie: Van cryptocurrency-diefstal tot technologische spionage

Noord-Korea speelt een centrale rol in internationale cyberdreigingen, met focus op financiële winst en technologische spionage. Groepen zoals Sapphire Sleet stelen grootschalig cryptocurrency, waaronder meer dan 10 miljoen dollar in zes maanden. Ze gebruiken geraffineerde social engineering, zoals nep-recruitment via platforms als LinkedIn, om slachtoffers te misleiden en malware te verspreiden.

Naast financiële aanvallen richt Ruby Sleet zich op de defensiesector met supply chain-aanvallen en malware die moeilijk te detecteren is. Hun doel is geavanceerde technologieën, zoals drones, voor militaire doeleinden te verkrijgen.

Een minder bekende strategie is het inzetten van Noord-Koreaanse IT-werkers die via platforms werken om intellectueel eigendom te stelen. Hun activiteiten worden ondersteund door facilitators die identiteitsvervalsing en toegang tot bedrijfsnetwerken mogelijk maken.

Organisaties kunnen zich beschermen door strengere controles, bewustwordingstrainingen en technologische maatregelen te implementeren. De dreigingen benadrukken de noodzaak van proactieve cyberbeveiliging.

Lees verder

Reading in ▯▯ or another language

Nijkerk - Helpdesk fraude

In januari 2024 werd een 69-jarige vrouw uit Nijkerk slachtoffer van bankmedewerkerfraude. Een oplichtster deed zich telefonisch voor als bankmedewerker en beweerde dat er een virus op haar bankpas zat. De vrouw werd overtuigd haar bankpas aan een koerier af te geven. De pas werd vervolgens misbruikt in diverse steden. De politie roept getuigen op om te helpen bij het identificeren van de verdachte.

Deze zaak benadrukt het belang van waakzaamheid tegen vormen van oplichting zoals vishing en smishing. Bij vishing gebruiken criminelen telefoontjes om persoonlijke gegevens te bemachtigen. Smishing werkt op dezelfde manier via sms. Ook tech support-scams en het misbruik van software zoals AnyDesk zijn populaire methoden van oplichters. Het advies blijft: deel nooit persoonlijke informatie via ongevraagde oproepen of berichten en blijf alert op verdachte

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

Maximaal te behalen **punten: 20**
Aantal deelnemers tot nu toe: 947 (+5)

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