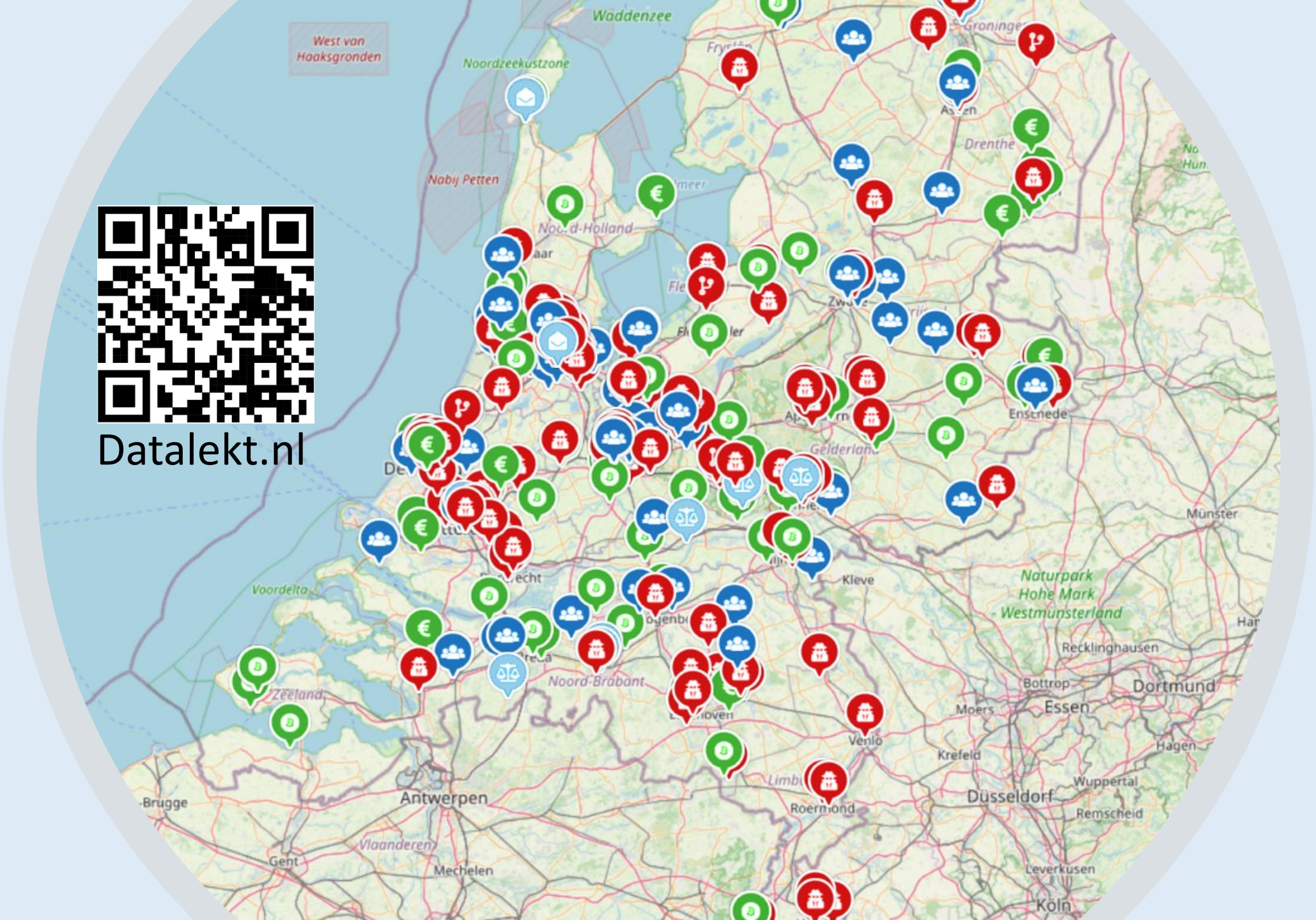
WELKOM BIJ

Festival CYBERSECURITY IN DE ZORG

Cybercrime & Privacy

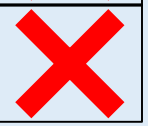
www.mariagenova.nl



- Adresgegevens duizenden studenten TU Eindhoven liggen op straat na hack ID-ware
- Bibliotheek Rotterdam kan door cyberaanval geen boeken uitlenen
- 120 Nederlandse tandartspraktijken tijdelijk dicht na cyberaanval, losgeld betaald
- Nederlandse windmolens al maanden stil door cyberaanvallen
- Datalek bij Farel College in Amersfoort: 1300 kinderen naar huis gestuurd
- OM: medewerkers Belastingdienst verkochten jarenlang data uit systemen
- Amsterdams festival DGTL lekt wachtwoorden en persoonsgegevens van 130.000 bezoekers
- Criminelen stalen creditcardgegevens door inbraak op site Intratuin

- Hackers verstoren reservatiesysteem bij InterContinental Hotels Group
- Datalek bij gemeente Groningen - mailadressen van honderden mensen in de bijstand op straat
- AIVD-medewerker verdacht van diefstal 102 computers
- KPN krijgt boete van 450.000 euro voor gebreken in beveiliging afluistersysteem
- Hackers vallen softwareleverancier van Gemeente Kerkrade aan
- Schoonmaakbedrijf CWS getroffen door cyberaanval
- Nepberichten verstuurd vanuit naam burgemeester van Den Helder
- Datalek politie na diefstal van documenten met persoonsgegevens uit auto

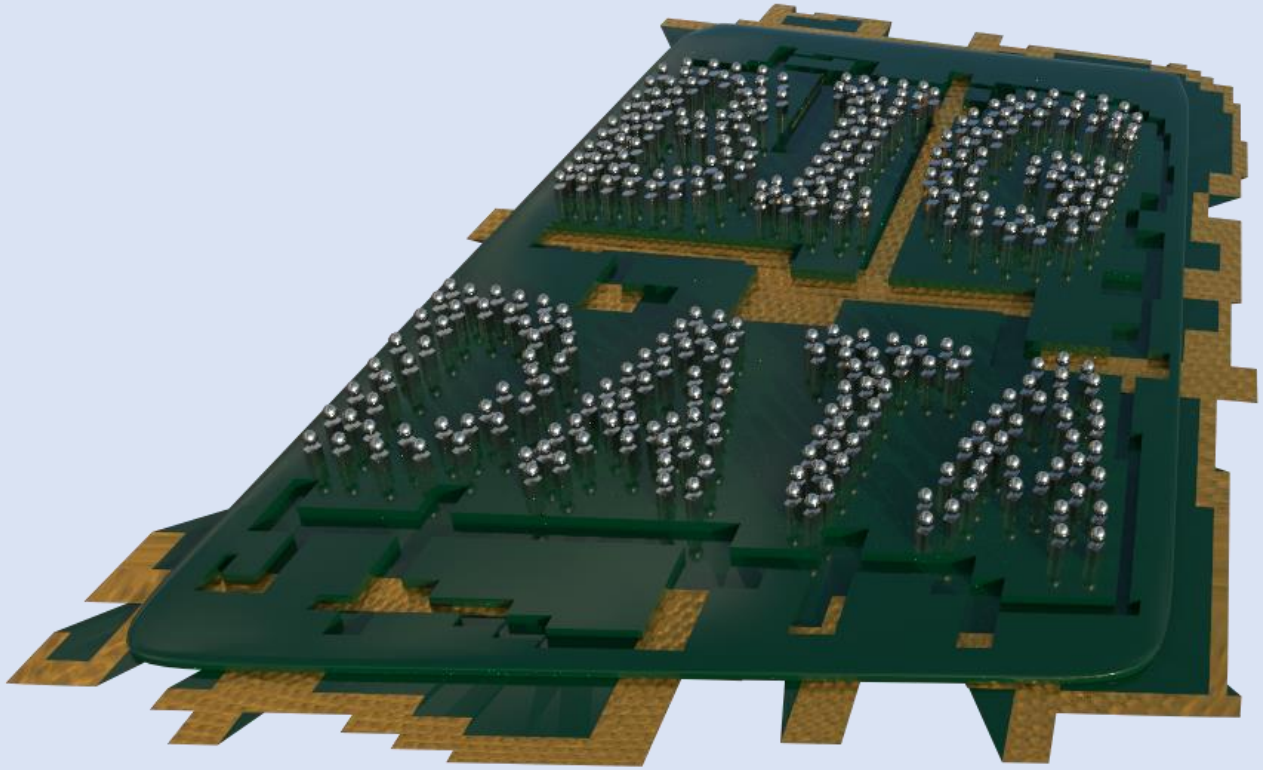
De mondzorg organisatie Colosseum Dental Benelux werd gehackt.

• A. De organisatie betaalde de hackers.	
• B. De organisatie weigerde te betalen en 120 praktijken bleven wekenlang dicht.	
• C. De organisatie betaalde niet, maar herstelde de klantinformatie vanuit back-ups.	

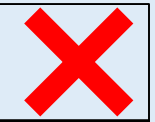
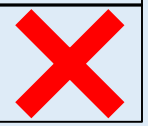
Via een aangesloten praktijk kwamen cybercriminelen in het netwerk van Colosseum Dental Benelux. Cruciale data werd gekaapt en versleuteld. Als gevolg hiervan moesten zo'n 120 Nederlandse tandartsenpraktijken tijdelijk hun deuren sluiten. De enige oplossing bleek de criminelen te betalen.

Trends

- Steeds meer data
- Lastiger te beschermen (meer dan 20.000 datalekken per jaar in Nederland)
- Kans op brand 1 op de 8000
- Kans op cyberaanval 1 op de 5
- Gemiddelde schade bij brand €14.000
- Gemiddelde schade bij cyberaanval €340.000



Wat is erger: thuis op een phishingmail klikken of op het werk?

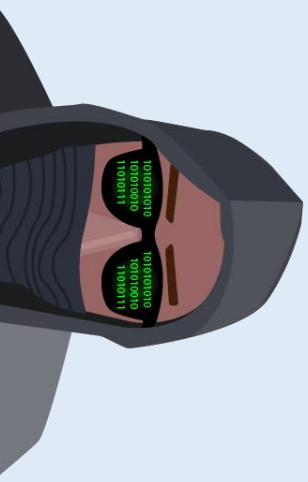
- A. Thuis, want er is niemand die je kan helpen. 
- B. Op het werk, ook al hebben we een IT-afdeling. 
- C. Het is allebei even erg. 

Antwoord B is juist. Qua omvang is een hack op een bedrijf vele malen erger dan op een individu. Alle computers kunnen op slot gezet worden en alle persoonlijk gegevens van klanten en medewerkers gestolen.

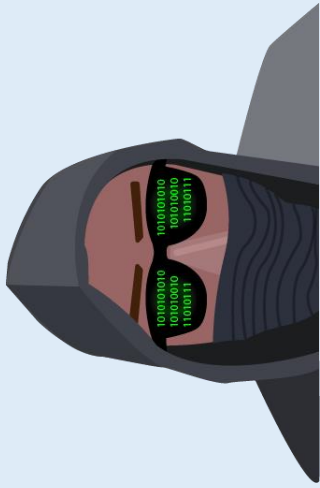
Gevolgen hacks en datalekken

- De helft van alle Nederlanders maakt jaarlijks een poging tot fraude mee.
- Een op de zes mensen raakt geld kwijt.
- In 2021 hebben we in Nederland in totaal 2,5 miljard euro overgemaakt aan online criminelen
- Jongeren worden vaker slachtoffer dan ouderen
- Ouderen raken veel hogere bedragen kwijt

Waarom hacken cybercriminelen steeds vaker kleine bedrijven?

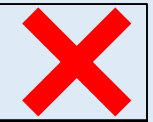


Moet een gehackt bedrijf bij afpersing betalen of niet?



Is een cyberverzekering wenselijk?

Wat deed ROC Mondriaan na een hack?

- A. Betaalde de hackers de gevraagde 4 miljoen euro om alles te herstellen. 
- B. Weigerde te betalen. Toen zetten de hackers de gegevens van 20.000 studenten en medewerkers te koop. 
- C. Herstelde zelf alles vanuit back-ups. Betaalde de hackers een kleiner bedrag om de gegevens niet te publiceren. 

Antwoord B. is juist. De scholengemeenschap weigerde om de hackers de gevraagde 4 miljoen euro te betalen. Daarom publiceerden de hackers allerlei vertrouwelijke informatie, van contactgegevens tot e-mails over schorsingen en van salarisstrookjes tot kopieën van identiteitsbewijzen.
ROC Mondriaan betaalde de slachtoffers die een nieuw identiteitsbewijs aanvroegen. Uiteraard kunnen veel gegevens nog steeds worden misbruikt voor identiteitsfraude.

Gemeente Hof van Twente werd volledig gehackt. Hoe kwamen de hackers binnen?

- A. Door een phishingmail. ✗
- B. Door het wachtwoord Welkom2020. ✓
- C. Door informatie die een medewerker op social media heeft gedeeld. ✗

Antwoord B is juist. Een systeembeheerder gebruikte het wachtwoord Welkom2020 voor een server voor externe toegang. Veel organisaties worden dagelijks aangevallen door hackers bij gemeente Hof van Twente was dat 50.000 tot 100 [illegible]r dag. De gemeente weigerde om het gevraagde losgeld te betalen. Alle data herstellen gaat naar verwachting ruim twee jaar kosten.

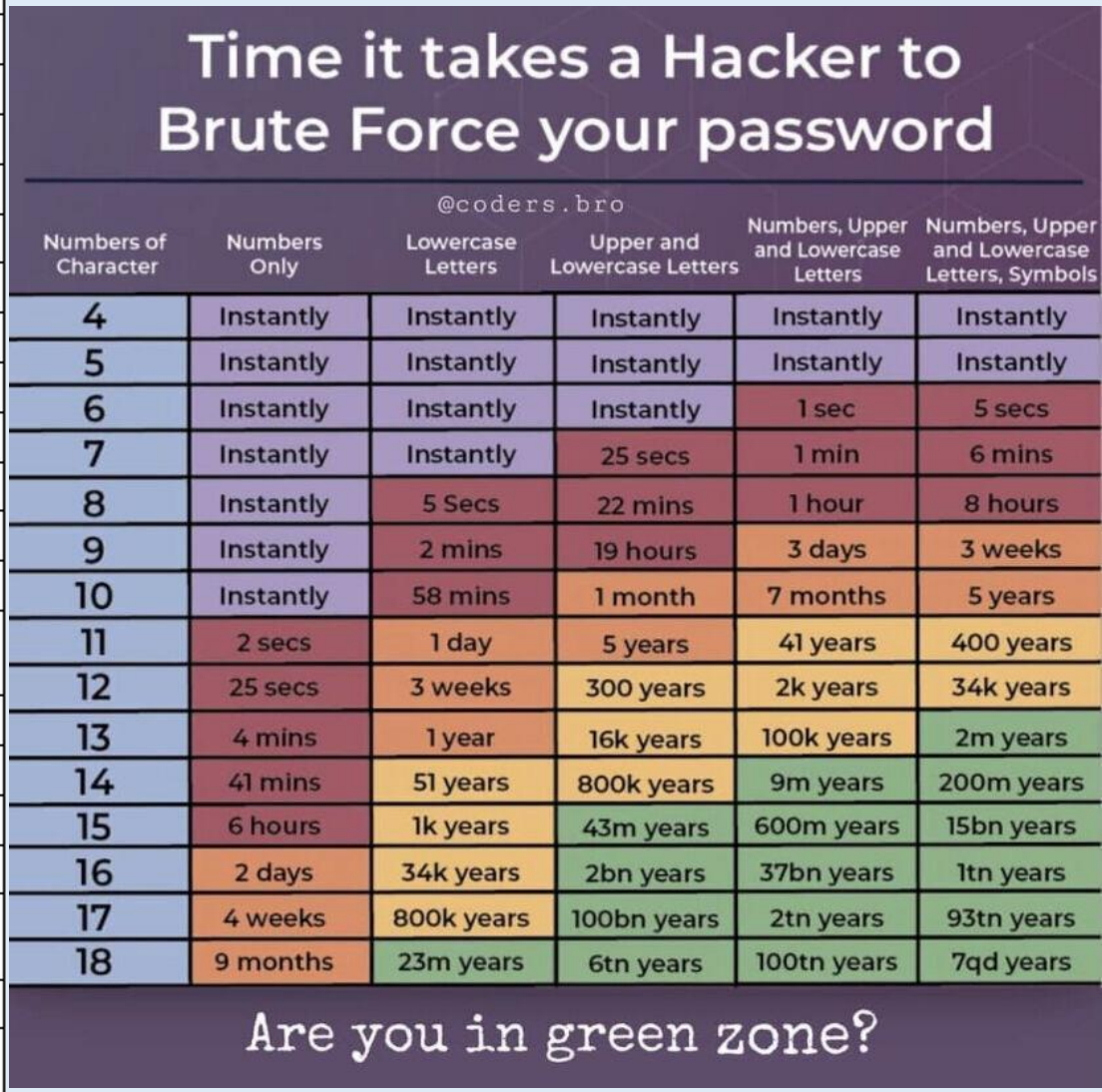
Is de zin 'Dit is een slecht wachtwoord’ sterk genoeg als wachtwoord als je het zo opschrijft: ditiseenslechtwachtwoord

• A. Ja, dit is een zeer sterk wachtwoord	✓
• B. Gemiddeld sterk	✗
• C. Dit is een zwak wachtwoord, want het bevat geen hoofdletter, cijfer of speciaal teken	✗

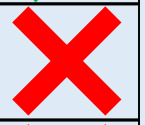
Antwoord A. is juist. Het is een misverstand dat sterke wachtwoorden niet alleen uit letters mogen bestaan. Kijk vooral naar de lengte van een wachtwoord. Boven die 14 karakters is het echt sterk. Deze zin bestaat uit meer dan 20 karakters en zo’n wachtwoord kun je in duizenden jaren niet hacken. Waarom willen zo veel websites dan wel dat je ook hoofdletters, cijfers en vreemde tekens gebruikt? Omdat veel mensen te korte wachtwoorden verzinnen en die zijn wel een stuk lastiger te hacken als ze complex zijn en niet alleen uit kleine letters bestaan. Bij lange wachtwoorden maakt dat niet uit.

Tip:
Gebruik een wachtwoordmanager zoals Bitwarden, LastPass of DashLane.

Slechtste wachtwoorden	Hoe lang om hem te kraken (volgens Random-ize)	Hoe lang om hem te kraken (volgens BetterBuys)
123546	Minder dan een seconde	0.25 milliseconden
123456789	Minder dan een seconde	0.25 milliseconden
qwerty	Minder dan een seconde	0.25 milliseconden
12345678	Minder dan een seconde	0.25 milliseconden
111111	Minder dan een seconde	0.25 milliseconden
1234567890	3 seconden	0.25 milliseconden
1234567	Minder dan een seconde	0.25 milliseconden
password	1 minuut, 13 seconden	0.25 milliseconden
123123	Minder dan een seconde	0.25 milliseconden
987654321	Minder dan een seconde	0.25 milliseconden
qwertyuiop	13 uur, 48 minuten	4 maanden, 4 dagen, 7 uur
mynoob	Minder dan een seconde	24 seconden
123321	Minder dan een seconde	0.25 milliseconden
666666	Minder dan een seconde	0.25 milliseconden
18atcskd2w	14 dagen, 21 uur	8 jaar, 9 maanden, 3 weken, 6 dagen, 8 uur
777777	Minder dan een seconde	0.25 milliseconden
1q2w3e4r	16 minuten, 33 seconden	0.25 milliseconden
654321	Minder dan een seconde	0.25 milliseconden
555555	Minder dan een seconde	2 minuten, 46 seconden
3rjs1la7qe	14 dagen, 21 uur	8 jaar, 9 maanden, 3 weken, 6 dagen, 8 uur
google	Minder dan een seconde	0.25 milliseconden
1q2w3e4r5t	14 dagen, 21 uur	8 jaar, 9 maanden, 3 weken, 6 dagen, 8 uur
123qwe	Minder dan een seconde	0.25 milliseconden
zxcvbnm	2 seconden	0.25 milliseconden
1q2w3e	Minder dan een seconde	0.25 milliseconden

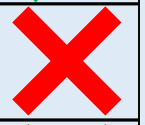


Cybercriminelen betalen geld voor advertenties.

- A. Feit. 
- B. Fabel. 
- C. Vast wel, maar betrouwbare sites weigeren dat soort advertenties. 

Antwoord A is juist. In een jaar tijd haalde Google meer dan tachtig miljoen frauduleuze advertenties offline. Zo leidde een advertentie van de Knab Bank naar een nagemaakte website en raakten klanten hun geld kwijt. Onderzoekers hebben ook advertenties ontdekt op boekhoudforums die boekhouders met virussen probeerden te infecteren. Nederland werd op een gegeven moment ook overspoeld met advertenties waarin bekende Nederlanders reclame maakten voor bitcoins. Dat was allemaal nep, de bekende Nederlanders wisten niet dat hun foto's misbruikt werden. Je zag die advertenties opduiken op Nu.nl, Marktplaats, YouTube, Facebook en Google en als je erop klikte, werd je geleid naar webpagina waar een winst van 2000% per dag werd beloofd. Veel mensen raakten al hun spaargeld kwijt.

De persoonlijke gegevens van zo’n 500 miljoen Facebook-gebruikers zijn te koop op een hackersforum.

- A. Ik wil weten of mijn telefoonnummer gelekt is en dan ga ik naar haveIbeenpwnd.com 
- B. De site haveibeenpwnd is betrouwbaar, maar daar kun je alleen checken of een wachtwoord gelekt is, niet en telefoonnummer. 
- C. Er is een tool waarmee je kunt checken of je telefoonnummer in handen is van hackers: ismijn06gelekt.nl 

Antwoord A. is juist. Eerst was de site haveIbeenpwnd alleen voor wachtwoorden, maar na de grote datalek van Facebook, met miljoenen telefoonnummers, werd het ook met een zoekfunctie op telefoonnummer uitgebreid. Meteen na het nieuws zag je allerlei tools verschijnen waarmee je dat ook kon checken. Sommige waren betrouwbaar, andere niet. ismijn06gelekt.nl lijkt te komen van iemand die het gevaar van dat soort tools laat zien. Log in met een vals telefoonnummer om te checken wat er gebeurt.

De site mijnING-online.nl is voorzien van een groen slotje en de site bankierenrabobank.nl niet. Wat zegt dat?

• A. Alleen de site met het groene slotje is veilig.	✗
• B. Ze zijn allebei onveilig.	✓
• C. Bankierenrabobank.nl klinkt niet betrouwbaar en dan maakt het groene slotje niets uit.	✗

Let op het groene slotje! Hoe vaak hoor je dat advie… …ls ook grif gebruik van een groen slotje. Duizenden websites beschikken over een werkend groen sloti… …e inloggegevens of besmetten je met een virus. Elke crimineel kan domeinnamen registreren die l… …NG-online.nl of bankierenrabobank.nl . Vroeger kostte het geld, daarom werd het niet zo vaak ged… …vragen en dat kan ook gratis. Een groen slotje betekent dat je op een veilige manier een verbindi… …r te verbinden met internetcriminelen. 'mijnING-online.nl ' lijkt best veel op de echte loginpa… …nil niet tussen een koppelteken en een punt. Je kunt er vanuit gaan dat een koppelteken vaak fout is, maar ook daar heb je uitzonderingen. Op… …s antwoord B juist: dit waren allebei foute sites met groene slotjes. Wat je in geval van twijfel moet doen? Het beste is om een site te googelen en niet via … link naar de site te gaan.

Veel voor de hand liggende sites met de namen van Nederlandse overheidsorganisaties zijn … …anden van derden. Veel andere domeinnamen met de naam van de organisatie erin, zijn nog steeds beschikbaar en te registreren voor slechts 1 euro per jaar. D… …bijvoorbeeld aan de toevoeging burgerzaken-(naam gemeente).nl of klantenservice-(naam organisatie).nl . Kwaadwillenden kunnen dat soort websites registrere… …betrouwbaar uitziende phishingmails met de logo van de organisatie versturen.

Van: DHL [mailto:no-reply@dhlparcel.com]
Verzonden: dinsdag 2 mei 2017 16:20
Aan:
Onderwerp: Levering gemist!

Beste Heer/Mevrouw,

Onze pakketbezorger heeft vandaag om 11:00 uur aan uw adres een pakket geprobeerd af te geven. Er was helaas niemand aanwezig om het pakket in ontvangst te kunnen nemen.

Uw pakket ligt klaar op een DHL ophaalpunt bij u in de buurt. Bekijk uw DHL Parcel informatie. Neem het ophaalbewijs uitgeprint mee naar het postkantoor. Vergeet niet om een geldig legitimatiebewijs (ID-Kaart, paspoort of rijbewijs) mee te nemen.

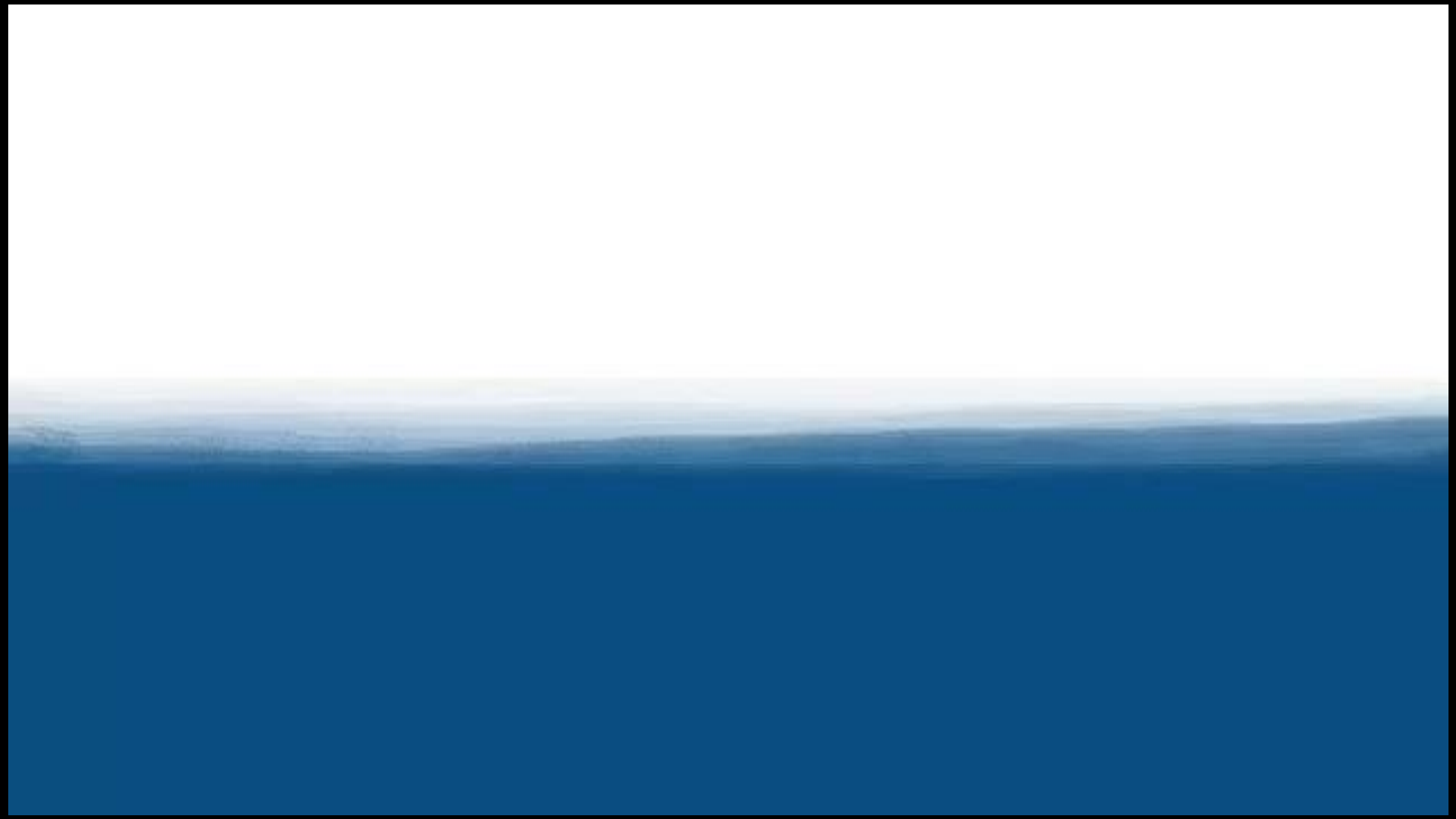
https://hoanggiangdigital.com/tracktrace.exe

De zending wordt veertien dagen na vandaag retour gestuurd, als het pakket niet opgehaald zal worden.

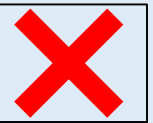
Kijk voor meer informatie over onze bezorgmogelijkheden op onze website

Met vriendelijke groet,

Cedric van de Berg
DHL Parcel



Een medewerker van Bol maakte 750.000 euro aan online oplichters. Wat was vreemd aan deze zaak?

- A. De medewerker trapte in een phishingmail, terwijl de afzender heel vreemd was. 
- B. De medewerker scande een kwaadaardige QR-code. 
- C. De medewerker maakte het geld over na een e-mail met ontelbare tikfouten. 

Antwoord C. is juist. De tekst van de mail was heel vreemd, met zinnen waar grammaticaal niets van klopte. Bol stapte naar de rechter omdat het bedrijf niet nog een keer ruim 750.000 euro wilde betalen. Maar de rechter oordeelde dat het niet uitmaakt dat Brabantia gehackt is, dus dat de mail van de juiste medewerkster leek te komen. De grammatica van de mail was heel slecht, een mix tussen Engels en Nederlands. Een rekeningnummer zonder enige controle wijzigen, is bovendien niet slim. Tekst e-mail: "Houd he rekening mee dat we vanaf vandaag een wijziging in onze bankrekeninggegevens hebben voor incaende betalingen", staat in de mail. "Voortaan moten all incoming betalingen have been overgemaakt naar onze filiaalrekening in Spanje. We het op prijs as u uw gegevens kunt bijwerken.” Na deze mail wijzigde Bol.com het rekeningnummer van Brabantia.

Je ontvangt een brief per post van je werkgever met een cadeaukaart voor je inzet. In de brief staat een QR-code.

- A. Ik scan de QR-code om de cadeaubon te verzilveren. 
- B. Zijn hackers op brieven overgestapt? Ik gooi de brief voor de zekerheid in de afvalbak. 
- C. Ik gebruik niet de QR-code, maar log zelf in op de website van MyGiftCard-Supply.com om de cadeaukaart te verzilveren. 

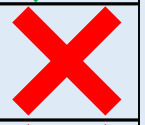
Antwoord B. is juist. Sommige hackers zijn inderdaad op fysieke brieven overgestapt. Namens werkgevers, namens de Belastingdienst, het waterschap, etc. Een QR-code kan leiden naar een website waar een virus op je staat te wachten. Voor de cadeaukaart moet je vaak inloggen met je zakelijke inloggegevens en daarmee kunnen ze soms je bedrijf of organisatie hacken. Als je zelf op de website inlogt, helpt dat ook niet, want je moet precies dezelfde gegevens invoeren en dan hebben de hackers ze ook binnen. MyGiftCard-Supply.com is trouwens niet meer online. De naam leek heel erg op dat van een bekend bedrijf in cadeaukaarten, met slechts één koppeltekentje verschil.

Tip:
Als je twijfelt, vraag altijd bij de werkgever na of iets klopt. Zeker als een website vraagt om in te loggen of gegevens in te voeren.

De belangrijkste maatregelen tegen cybercrime

- Offline back-ups
- Wachtwoordbeleid, Multi-factor authenticatie (MFA)
- Patch beleid (wie is verantwoordelijk voor de updates)
- Hoeveel updates moeten er op dat moment nog uitgevoerd worden?
- Welke leveranciers hebben toegang tot het systeem?
- Welke persoonlijke gegevens worden bewaard?
- Hoe lang worden persoonlijke gegevens bewaard en met welk doel?
- Evaluatie belangrijkste data
- Wie heeft toegang tot de belangrijkste data?
- Calamiteitenplan

Een op de acht Nederlanders bestelde vorig jaar bij een nep webshop. Wie trapten er vaker in: mannen of vrouwen?

- A. Mannen. 
- B. Vrouwen. 
- C. Geslacht maakt niet veel uit. 

Uit onderzoek van creditcardmaatschappij ICS bleek dat mannen twee keer zo vaak producten bij een nepwinkel bestelden als vrouwen. Soms gaat het om onbekende webwinkels, maar het gebeurt ook dat webwinkels van gerenommeerde bedrijven worden nagemaakt. Tegen de tijd dat een klant doorkrijgt dat hij bedonderd is, is de webwinkel alweer verdwenen.

Website: mariagenova.nl

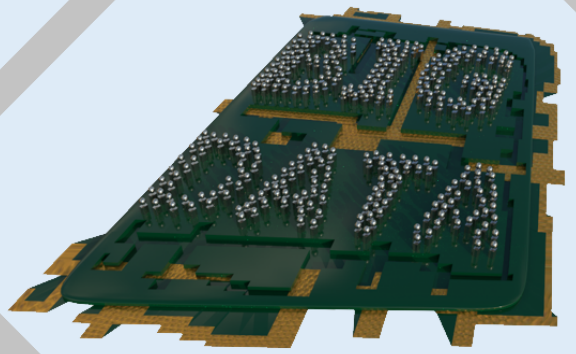
Email: genova@casema.nl

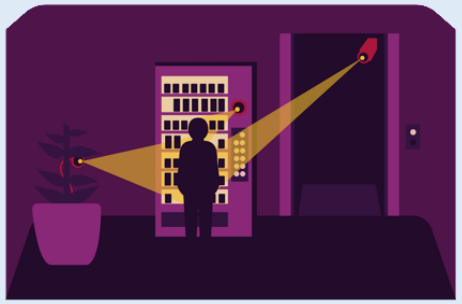
Twitter: Genova2

Instagram: Genova2000

LinkedIn: Maria Genova

Cybercrimetips.nl





Festival CYBERSECURITY IN DE ZORG

ACUTEZORG EUREGIO
ZorgNetOost
Centrum voor Veiligheid en Digitalisering
Spoedzorg Huisartsen Twente
Thoon
UNIVERSITY OF TWENTE.
Federatie Eerstelijnzorg Almelo e.o.
SAXION