DELL Technologies

Bent u slimmer dan uw cybercrimineel?

Quiz starten

VRAAG 1 VAN 14

Phishing

U ontvangt een e-mail van ‘Windows Defender Order’ met een factuur die er officieel uitziet voor $ 399,99 voor een 1-jarig abonnement op een account van Microsoft Defender. Er staat duidelijk ‘Gelieve niet te reageren op deze e-mail’, maar er staat wel een knop ‘Help & Contact’ en een telefoonnummer. U kunt zich niet herinneren dat u zoiets hebt besteld.

Wat doet u?

Nr. 1

Selecteer hieronder het beste antwoord

A U klikt op de knop ‘Help & Contact’ want u wilt natuurlijk niet dat dit bedrag van uw creditcard wordt afgeschreven!

B U opent de e-mail in een incognitovenster in de webbrowser en klikt dan op de knop ‘Help & Contact’.

C U controleert uw online creditcardafschrift om te zien of het bedrag is afgeschreven. Daarna gebruikt u het telefoonnummer om meer informatie te verkrijgen.

D U controleert het e-mailadres en realiseert zich dat het er verdacht uitziet, dus u klikt op ‘Phishing rapporteren’ via uw mailprogramma en/of stuurt de mail door naar uw IT-afdeling voor onderzoek. En natuurlijk opent u de mail niet!

E U verwijdert de mail zonder deze te openen.

DELL Technologies

ANTWOORD

Phishing

Nr. 1

GOED GEDAAN!

Phishing rapporteren!

Wanneer u een verdachte e-mail ontvangt waarin u om welke reden dan ook wordt gevraagd op een link te klikken, kunt u de e-mail het beste verwijderen zonder deze te openen of op ‘Phishing rapporteren’ in uw Outlook-balk klikken om deze voor onderzoek naar IT te sturen. **Als u het verdacht vindt, is dat het meestal ook.**

Volgende vraag

DELL Technologies

ANTWOORD

Phishing

Nr. 1

GOED GEDAAN, MAAR...

Phishing rapporteren!

U brengt uzelf nog steeds in gevaar door een nep telefoonnummer te bellen. Een van de andere opties in deze lijst is een betere oplossing. **Als u het verdacht vindt, is dat het meestal ook.**

Volgende vraag

DELL Technologies

ANTWOORD

Phishing

Nr. 1

GEHACKT!!!

Phishing rapporteren!

Onthoud dat wanneer u een verdachte e-mail ontvangt waarin u om welke reden dan ook wordt gevraagd op een link te klikken, u de e-mail het beste kunt verwijderen zonder deze te openen of op ‘Phishing rapporteren’ in uw Outlook-balk kunt klikken om deze voor onderzoek naar IT te sturen.
Als u het verdacht vindt, is dat het meestal ook.

Volgende vraag

DELL Technologies

VRAAG 2 VAN 14

Phishing op sociale media

U bekijkt uw Instagram account, en Lyle Lovett heeft direct gereageerd op uw opmerking bij zijn posts! Hij vraagt u om contact te leggen via een rechtstreeks bericht, en stuurt u een link waarop u moet klikken om toegang te krijgen tot zeer beperkte en waardevolle content.

U:

Nr. 2

Selecteer hieronder het beste antwoord

A Kunt uw geluk niet op en klikt onmiddellijk op de link.

B Kopieert de link en opent deze in een incognitovenster.

C Deelt de link op sociale media met uw vrienden.

D Zweeft met uw muis over de link en hebt het gevoel dat er iets mis is. Daarom verwijdert u het bericht en blokkeert u de zender.

E Blokkeert en rapporteert de afzender zonder op iets te klikken.

DELL Technologies

ANTWOORD

Phishing op sociale media

Nr. 2

GOED GEDAAN!

Phishing rapporteren!

Wanneer u een verdachte e-mail ontvangt waarin u om welke reden dan ook wordt gevraagd op een link te klikken, kunt u de e-mail het beste verwijderen zonder deze te openen of op ‘Phishing rapporteren’ in uw Outlook-balk klikken om deze voor onderzoek naar IT te sturen. **Als u het verdacht vindt, is dat het meestal ook.**

Volgende vraag

DELL Technologies

ANTWOORD

Phishing op sociale media

Nr. 2

GEHACKT!!!

Phishing rapporteren!

Onthoud dat wanneer u een verdachte e-mail ontvangt waarin u om welke reden dan ook wordt gevraagd op een link te klikken, u de e-mail het beste kunt verwijderen zonder deze te openen of op ‘Phishing rapporteren’ in uw Outlook-balk kunt klikken om deze voor onderzoek naar IT te sturen. **Als u het verdacht vindt, is dat het meestal ook.**

Volgende vraag

DELL Technologies

VRAAG 3 VAN 14

Wachtwoordbeveiliging

Uw IT-afdeling dringt erop aan om sterke wachtwoorden aan te maken. De reden hiervoor is dat deze ‘inloggegevens’ een van de meest gewilde doelen zijn van aanvallers. Dus...

Hoe kunt u uw wachtwoord veiliger maken?

Nr. 3

Selecteer hieronder het beste antwoord

A	Door minstens 8 tekens en liever meer te gebruiken.
B	Door een combinatie van letters, cijfers en tekens te gebruiken.
C	Door niet hetzelfde wachtwoord voor meerdere accounts of websites te gebruiken (u maakt telkens een uniek wachtwoord aan).
D	Alle bovenstaande opties.
E	Geen van bovenstaande opties.

DELL Technologies

ANTWOORD

Wachtwoordbeveiliging

Nr. 3

GOED GEDAAN!

Gebruik een sterk wachtwoord!

Een veilig wachtwoord is uniek en bestaat ten minste uit 8 letters, cijfers en tekens. Misschien is het zelfs een unieke wachtzin die u kunt onthouden. En gebruik niet de naam van uw hond! Probeer ook gebruik te maken van tweevoudige verificatie. Dit plus een sterk wachtwoord is garantie voor optimale bescherming.

Volgende vraag

DELL Technologies

ANTWOORD

Wachtwoordbeveiliging

Nr. 3

GOED GEDAAN, MAAR...

Gebruik een sterk wachtwoord!

Een veilig wachtwoord combineert alle beveiligingsmaatregelen die vermeld zijn: het is uniek en bevat ten minste 8 letters, cijfers en tekens. En gebruik niet de naam van uw hond! Voor aanvullende beveiliging kunt u tweevoudige verificatie en wachtzinnen met cijfers en tekens gebruiken in plaats van wachtwoorden.

Volgende vraag

DELL Technologies

ANTWOORD

Wachtwoordbeveiliging

Nr. 3

GEHACKT!!!

Gebruik een sterk wachtwoord!

Een veilig wachtwoord is uniek en bevat ten minste 8 letters, cijfers en tekens. Voor aanvullende beveiliging kunt u tweevoudige verificatie en wachtzinnen met cijfers en tekens gebruiken in plaats van wachtwoorden.

Volgende vraag

DELL Technologies

VRAAG 4 VAN 14

Social engineering

U wordt gebeld op uw mobiel door iemand die beweert dat hij van uw IT-afdeling is. Deze persoon vertelt u dat uw wachtwoord is verlopen en dat u een nieuw wachtwoord moet instellen. Het telefoonnummer ziet er veilig uit. U wordt gevraagd om uw personeelsnummer, BSN-nummer en geboortedatum ter verificatie.

Wat doet u?

Nr. 4

Selecteer hieronder het beste antwoord

A U verstrekt uw gegevens, want u wilt u wachtwoord opnieuw instellen en terug aan het werk.

B U vraagt om hun contactgegevens, zoals e-mailadres en telefoonnummer, om hun identiteit te controleren. Daarna verstrekt u de gevraagde gegevens.

C U verbreekt onmiddellijk de verbinding en rapporteert het telefoontje bij uw IT-afdeling.

D U verstrekt uw personeelsnummer en geboortedatum, maar niet uw BSN-nummer.

E Geen van bovenstaande opties.

DELL Technologies

ANTWOORD

Social engineering

Nr. 4

GOED GEDAAN!

Verbreek de verbinding en neem contact op met IT!

Sommige aanvallers gebruiken social engineering om u te manipuleren uw gevoelige gegevens te delen via de telefoon. Zelfs als u in uw systeem kunt controleren of iemand een werknemer is, betekent dit nog niet dat u ook echt met deze persoon spreekt. **U moet altijd zelf uw wachtwoorden opnieuw instellen.**

Volgende vraag

DELL Technologies

ANTWOORD

Social engineering

Nr. 4

GEHACKT!!!

Verbreek de verbinding en neem contact op met IT!

Sommige aanvallers gebruiken social engineering om u te manipuleren uw gevoelige gegevens te delen via de telefoon. Zelfs als u in uw systeem kunt controleren of iemand een werknemer is, betekent dit nog niet dat u ook echt met deze persoon spreekt.
U moet altijd zelf uw wachtwoorden opnieuw instellen.

Volgende vraag

DELL Technologies

VRAAG 5 VAN 14

Infiltratie op uw pc

Terwijl u aan de lijn bent, bemerkt u vreemd gedrag op uw scherm, zoals de muis die uit zichzelf beweegt, tekst- of consolevensters die openen en sluiten, of menu's die open- en dichtklappen.

Dus:

Nr. 5

Selecteer hieronder het beste antwoord

A U gaat ervan uit dat het een onschuldig pc-probleem is en werkt door.

B U vraagt het even na bij uw IT-afdeling, maar ondertussen werkt u gewoon door.

C U stopt onmiddellijk met het gebruik van uw pc en sluit deze af. Daarna neemt u contact op met uw IT-afdeling (via een ander apparaat) om het probleem te melden.

DELL Technologies

ANTWOORD

Infiltratie op uw pc

Nr. 5

GOED GEDAAN!

Neem onmiddellijk contact op met IT!

Als uw muis ‘uit zichzelf’ over het scherm beweegt, kan dit wijzen op een ernstige aanval met data-inbreuk en mogelijk keylogging. U moet uw IT-afdeling onmiddellijk op de hoogte stellen zodat ze er goed op kunnen reageren.

Volgende vraag

DELL Technologies

ANTWOORD

Infiltratie op uw pc

Nr. 5

GEHACKT!!!

Neem onmiddellijk contact op met IT!

Abnormaal gedrag kan erop wijzen dat een aanvaller uw pc in de gaten houdt, en mogelijk zowel gegevens exfiltreert als toetsaanslagen vastlegt, waaronder uw wachtwoorden en andere kritieke informatie. De beste optie is om uw pc onmiddellijk uit te schakelen en het probleem te melden bij uw IT-afdeling.

Volgende vraag

DELL Technologies

VRAAG 6 VAN 14

Malware-aanval via USB

Terwijl u over de parkeerplaats van uw bedrijf loopt, ziet u tussen twee auto's een boodschappentasje liggen. U ontdekt dat er vijf USB-sticks nog ongeopend in de originele verpakking zitten met elk 500 GB opslag!

Wat doet u?

Nr. 6

Selecteer hieronder het beste antwoord

A U opent er één en steekt deze in de USB-poort van uw pc. De andere vier geeft u weg aan uw collega's.

B U neemt ze mee naar huis en gebruikt de USB-sticks op uw pc.

C U brengt de beveiliging van het kantoor en uw IT-afdeling op de hoogte en geeft de USB-sticks aan hen.

D U geeft de USB-sticks weg als cadeau aan uw kinderen voor de kerst.

E Geen van bovenstaande opties.

DELL Technologies

ANTWOORD

Malware-aanval via USB

Nr. 6

GOED GEDAAN!

Breng de beveiliging en IT op de hoogte!

Met dit soort aanvallen kan een crimineel malware binnenbrengen in een organisatie, waarbij een werknemer als ‘mule’ wordt gebruikt om de schadelijke payload in het netwerk in te brengen. Steek NOOIT een USB-stick of een andere accessoire van onbekende herkomst in een apparaat dat van u is. En het zijn geen leuke cadeautjes!

Volgende vraag

DELL Technologies

ANTWOORD

Malware-aanval via USB

Nr. 6

GEHACKT!!!

Breng de beveiliging en IT op de hoogte!

Met dit soort aanvallen kan een crimineel malware binnenbrengen in een organisatie, waarbij een werknemer als ‘mule’ wordt gebruikt om de schadelijke payload in het netwerk in te brengen. Steek NOOIT een USB-stick of een andere accessoire van onbekende herkomst in een apparaat dat van u is. En het zijn geen leuke cadeautjes!

Volgende vraag

DELL Technologies

VRAAG 7 VAN 14

Ransomware

Een verkoper komt naar uw kantoor om een presentatie te geven over een nieuwe technologie die uw bedrijf wil aanschaffen. De verkoper brengt de presentatie mee op een USB-stick en vraagt u deze in uw pc te steken zodat de presentatie kan worden geprojecteerd tijdens het praatje.

Wat doet u?

Nr. 7

Selecteer hieronder het beste antwoord

A U doet wat diegene vraagt en steekt de USB-stick in uw pc.

B U vraagt of de presentatie niet ook gedownload kan worden, omdat uw bedrijf het gebruik van externe USB-sticks verbiedt. Als er echter geen mogelijkheid is om te downloaden, doet u alsnog wat de verkoper vraagt en steekt u de USB-stick in uw pc.

C U vraagt de verkoper om de presentatie te houden zonder de projectie en steekt de USB niet in uw pc.

D U vraagt na of ze de USB-stick niet ergens hebben gevonden en steekt deze daarna in uw pc.

E U maakt extra kopieën van de USB-stick en geeft er een aan uw manager.

DELL Technologies

ANTWOORD

Ransomware

Nr. 7

GOED GEDAAN!

Steek de USB-stick niet in uw pc.

Zonder dat u het wist is de verkoper omgekocht door een aanvaller en bevat de USB-stick een ransomware payload die uw systemen vergrendelt. Doordat u de USB-stick niet hebt aangesloten en geen andere bestanden hebt gedownload, hebt u voorkomen dat de aanvaller toegang kreeg. Oef!

Volgende vraag

DELL Technologies

ANTWOORD

Ransomware

Nr. 7

GEHACKT!!!

Steek de USB-stick niet in uw pc.

Zonder dat u het wist is de verkoper omgekocht door een aanvaller. De USB-stick en het gedownloade bestand bevatten een ransomware payload die uw systemen vergrendelt. Vermijd het gebruik van externe USB-sticks en het downloaden van bestanden van onbekende herkomst op persoonlijke of zakelijke pc's.

Volgende vraag

DELL Technologies

VRAAG 8 VAN 14

Tweevoudige verificatie

Uw bank heeft u aangeraden tweevoudige verificatie te gebruiken wanneer u inlogt op hun site. Andere websites maken ook gebruik van dit proces om de veiligheid van de gebruiker te garanderen.

Welke van de onderstaande situaties is een voorbeeld van tweevoudige verificatie?

Nr. 8

Selecteer hieronder het beste antwoord

A U voert uw gebruikersnaam en wachtwoord in. Daarna wordt u gevraagd om uw pincode in te voeren om toegang te krijgen tot de website.

B U voert uw gebruikersnaam en wachtwoord in, plus een CAPCHA waarbij u panelen ontcijfert met de tekens.

C U voert uw gebruikersnaam en wachtwoord in en de website stuurt een sms naar uw mobiele telefoon met een eenmalige code die u invoert in het daarvoor bestemde vakje op de website.

D U voert uw gebruikersnaam in, en de website vereist dat u een code invoert van een beveiligd token dat elke minuut verandert en dat op uw telefoon is geïnstalleerd.

E Alleen A en C.

F Alleen C en D.

G Geen van bovenstaande opties.

DELL Technologies

ANTWOORD

Tweevoudige verificatie

Nr. 8

GOED GEDAAN!

U hebt beide nodig!

Tweevoudige verificatie vereist zowel een wachtwoord als een tweede, andere identificatiecode, zoals een code die per sms wordt verzonden of een nummer dat door een app wordt gegenereerd, om gebruikers te identificeren en te verifiëren. Deze beveiligingslaag maakt het veel moeilijker voor aanvallers om toegang te krijgen tot uw informatie.

Volgende vraag

DELL Technologies

ANTWOORD

Tweevoudige verificatie

Nr. 8

GOED GEDAAN, MAAR...

U hebt beide nodig!

U zit in de buurt! Er zijn hier twee voorbeelden van tweevoudige verificatie. Probeer het opnieuw en kijk of u de andere kunt herkennen.

Volgende vraag

DELL Technologies

ANTWOORD

Tweevoudige verificatie

Nr. 8

GEHACKT!!!

Oeps! U hebt beide nodig!

Tweevoudige verificatie vereist zowel een wachtwoord als een tweede, andere identificatiecode, zoals een code die per sms wordt verzonden of een nummer dat door een app wordt gegenereerd, om gebruikers te identificeren en te verifiëren. Deze beveiligingslaag maakt het veel moeilijker voor aanvallers om toegang te krijgen tot uw informatie. Als u hier geen gebruik van maakt bent u kwetsbaar voor aanvallers.

Volgende vraag

DELL Technologies

VRAAG 9 VAN 14

Bluetooth dieven

Nadat u met de auto naar een wandelroute bent gereden om een middag lekker te wandelen, ontdekt u dat uw laptop nog in uw rugtas zit. Ook hebt u uw telefoon bij u (die hier geen bereik heeft). U wilt uw computer en telefoon in de auto achterlaten, maar wilt wel dat ze veilig zijn.

Wat doet u?

Nr. 9

Selecteer hieronder het beste antwoord

A U schakelt alle wifi uit.

B U zet uw laptop in de slaapstand.

C U legt uw laptop en telefoon in de achterbak en sluit deze af.

D U wikkelt uw laptop en telefoon in een dikke deken.

E U zet uw laptop en telefoon helemaal uit, waardoor Bluetooth ook wordt uitgeschakeld.

DELL Technologies

ANTWOORD

Bluetooth dieven

Nr. 9

GOED GEDAAN!

Zet uw laptop en telefoon uit!

Hoewel het altijd goed is om apparaten uit het zicht te houden wanneer u er niet bij bent, kunnen dieven ook gebruik maken van Bluetooth-scanners om apparaten in afgesloten voertuigen te lokaliseren. Niet alle apparaten schakelen Bluetooth uit in de slaapstand. Diefstallen vinden vaak plaats bij de start van wandelroutes of andere locaties waar eigenaren vaak langere tijd weg zijn. En dieven houden alles in de gaten! Dus wees voorzichtig als u gaat wandelen!

Volgende vraag

DELL Technologies

ANTWOORD

Bluetooth dieven

Nr. 9

GEHACKT!!!

Zet uw laptop en telefoon uit!

Hoewel het altijd goed is om apparaten uit het zicht te houden wanneer u er niet bij bent, kunnen dieven ook gebruik maken van Bluetooth-scanners om apparaten in afgesloten voertuigen te lokaliseren. Niet alle apparaten schakelen Bluetooth uit in de slaapstand. Diefstallen vinden vaak plaats bij de start van wandelroutes waar eigenaren vaak langere tijd weg zijn. Wees dus voorzichtig als u gaat wandelen!

Volgende vraag

DELL Technologies

VRAAG 10 VAN 14

Aanval via USB: deel 2

Omdat u in de feeststeer zit, neemt u een minikerstboompje met USB-aansluiting mee om uw kantoor te versieren.

Hoe sluit u dit aan?

Nr. 10

Selecteer hieronder het beste antwoord

A U sluit de kerstboom aan via uw pc.

B U sluit de kerstboom aan via een USB-verlengstuk dat aangesloten is op uw pc.

C U gebruikt een speciale USB-adapter om het apparaat in een normaal stopcontact te steken.

D Er is geen goede manier om de kerstboom aan te sluiten. Kerst gaat niet door.

E Geen van bovenstaande opties.

DELL Technologies

ANTWOORD

Aanval via USB: deel 2

Nr. 10

GOED GEDAAN!

Gebruik een speciale USB-adapter!

Deze variant van aanvallen via USB wordt vaak gebruikt om malware op apparaten te krijgen, zelfs via kleine kerstboompjes! In de hoop dat ze uiteindelijk worden aangesloten op het netwerk van een waardevol bedrijf. Steek nooit een onbekend USB-apparaat in uw pc, zelfs niet om het alleen op te laden.

Volgende vraag

DELL Technologies

ANTWOORD

Aanval via USB: deel 2

Nr. 10

GEHACKT!!!

Gebruik een speciale USB-adapter!

Deze variant van aanvallen via USB wordt vaak gebruikt om malware op apparaten te krijgen, zelfs via kleine kerstboompjes! In de hoop dat ze uiteindelijk worden aangesloten op het netwerk van een waardevol bedrijf. Steek nooit een onbekend USB-apparaat in uw pc, zelfs niet om het alleen op te laden.

Volgende vraag

DELL Technologies

VRAAG 11 VAN 14

Gevaarlijke schoonmaakster

U verblijft in een vijfsterrenhotel in Shanghai, China, vanwege een conferentie over cyberveiligheid. Voordat u gaat eten, stopt u de pc in de kluis van uw hotelkamer.

Is uw pc veilig tegen aanvallen en diefstal?

Nr. 11

Selecteer hieronder het beste antwoord

A Nee, want elk apparaat dat onbewaakt achter wordt gelaten kan gehackt worden.

B Ja, want u hebt het veilig opgeborgen in de kluis.

C Ja, want u hebt ook nog kleding in de kast gehangen om de kluis te verbergen.

D Ja, want het is een heel mooi hotel.

E Ja, want het is niet eens een hele mooie pc.

DELL Technologies

ANTWOORD

Gevaarlijke schoonmaakster

Nr. 11

GOED GEDAAN!

Nee, elk apparaat kan worden gehackt!

Elk apparaat dat onbewaakt achter wordt gelaten kan worden geopend en gecompromitteerd via wat algemeen bekend staat als de ‘Evil Maid’ aanval. Hierbij krijgt de aanvaller toegang door de pc fysiek te openen en de malware in te brengen. Een apparaat dat niet fysiek onder uw hoede is, is kwetsbaar voor aanvallen. Laat onbekende personen ook nooit op uw apparaat passen, vooral niet als het een gevaarlijke schoonmaakster betreft.

Volgende vraag

DELL Technologies

ANTWOORD

Gevaarlijke schoonmaakster

Nr. 11

GEHACKT!!!

Nee, elk apparaat kan worden gehackt!

Elk apparaat dat onbewaakt achter wordt gelaten kan worden geopend en gecompromitteerd via wat algemeen bekend staat als de ‘Evil Maid’ aanval. Hierbij krijgt de aanvaller toegang door de pc fysiek te openen en de malware in te brengen. Om echt veilig te zijn moet u elk apparaat bij u houden. Laat onbekende personen nooit op uw apparaat passen, vooral niet als het een gevaarlijke schoonmaakster betreft.

Volgende vraag

DELL Technologies

VRAAG 12 VAN 14

Spyware

U krijgt een sms van een vaag bekend nummer waarin staat dat uw dochter een ongeluk heeft gehad en in het ziekenhuis ligt. In het sms'je staat een link waarmee u onmiddellijk contact kunt leggen.

U:

Nr. 12

Selecteer hieronder het beste antwoord

A	Klikt onmiddellijk op de link want u bent bezorgd over uw dochter.
B	Zoekt het nummer op, ontdekt dat het uit het gebied komt waar uw dochter was en klikt daarna op de link.
C	Klikt niet op de link en sms't in plaats daarvan uw dochter om te vragen of alles goed is.
D	Geen van bovenstaande opties.

DELL Technologies

ANTWOORD

Spyware

Nr. 12

GOED GEDAAN!

Klik niet op de link!

Bij dit soort aanvallen wordt er geprobeerd om spyware op uw telefoon te plaatsen. Hierdoor kan uw telefoon aangetast worden en de spyware kan zelfs verder verspreid worden naar uw bedrijfsnetwerk. U herkende iets verdachts en gebruikte een andere methode om te controleren of alles goed was met uw dochter. Goed gedaan!

Volgende vraag

DELL Technologies

ANTWOORD

Spyware

Nr. 12

GEHACKT!!!

Klik niet op de link!

Bij dit soort aanvallen wordt er geprobeerd om spyware op uw telefoon te plaatsen. Hierdoor kan uw telefoon aangetast worden en de spyware kan zelfs verder verspreid worden naar uw bedrijfsnetwerk. Door op de link te klikken wordt er spyware payload op uw apparaat gezet. Laat u niet verleiden door vreemde sms'jes hoe verleidelijk dit ook kan zijn.

Volgende vraag

DELL Technologies

VRAAG 13 VAN 14

Beveiliging van eindpunten

Kwaadwillende figuren (ook wel hackers met kwade bedoelingen) richten zich op eindpunten.

De definitie van eindpunten is:

Nr. 13

Selecteer hieronder het beste antwoord

A	Desktops.
B	Desktops en notebooks.
C	Desktops, notebooks en servers.
D	Desktops, notebooks, servers, de cloud en meer.
E	Desktops, notebooks, servers, de cloud en de laatste bestemming op mijn TomTom.

DELL Technologies

ANTWOORD

Beveiliging van eindpunten

Nr. 13

GOED GEDAAN!

Elk apparaat dat op afstand is verbonden!

Een eindpunt is een apparaat dat op afstand verbonden is met een netwerk. Eindpuntbeveiliging is cruciaal voor de bescherming van apparaten en data in uw organisatie, dus zorg dat u aanvallers een stap voor blijft!

Volgende vraag

DELL Technologies

ANTWOORD

Beveiliging van eindpunten

Nr. 13

GOED GEDAAN, MAAR...

Elk apparaat dat op afstand is verbonden!

Een eindpunt is een apparaat dat op afstand verbonden is met een netwerk. Eindpuntbeveiliging is cruciaal voor de bescherming van apparaten en data in uw organisatie, dus zorg dat u aanvallers een stap voor blijft!

Volgende vraag

DELL Technologies

ANTWOORD

Beveiliging van eindpunten

Nr. 13

GEHACKT!!!

Elk apparaat dat op afstand is verbonden!

Een eindpunt is een apparaat dat op afstand verbonden is met een netwerk. Eindpuntbeveiliging is cruciaal voor de bescherming van apparaten en data in uw organisatie, dus zorg dat u aanvallers een stap voor blijft!

Volgende vraag

DELL Technologies

VRAAG 14 VAN 14

Eindpuntbeveiliging: deel 2

Hackers met kwade bedoelingen richten zich op eindpunten, zoals desktops, laptops, mobiele telefoons, draadloze printers en servers, ofwel alles wat verbinding maakt met een netwerk.

Welke stappen kunt u nemen om een aanval te voorkomen?

Nr. 14

Selecteer hieronder het beste antwoord

A Ik zorg dat ik mijn apparaat vergrendel en opberg als ik het niet gebruik.

B Ik update en patch mijn apparaat regelmatig.

C Ik zorg dat ik mijn inbox schoonhoud: meld verdachte e-mails.

D Ik sluit nooit een onbekend apparaat aan op mijn eindpunt.

E Alle bovenstaande opties.

DELL Technologies

ANTWOORD

Eindpuntbeveiliging: deel 2

Nr. 14

GOED GEDAAN!

Alle bovenstaande opties!

U hebt geleerd hoe u cyberveilig kunt zijn en zet dit ook in de praktijk. Eindpuntbeveiliging is cruciaal voor de bescherming van apparaten en data in uw organisatie, dus zorg dat u aanvallers een stap voor blijft!

Volgende vraag

DELL Technologies

ANTWOORD

Eindpuntbeveiliging: deel 2

Nr. 14

GOED GEDAAN, MAAR...

U kunt nog meer doen!

Er zijn nog meer dingen die u kunt doen om uw apparaten te beschermen. Eindpuntbeveiliging is cruciaal voor de bescherming van apparaten en data in uw organisatie, dus zorg dat u aanvallers een stap voor blijft!

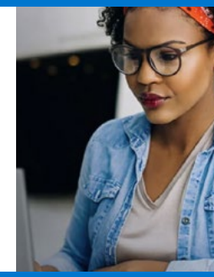
Volgende vraag

DELL Technologies

HARTELIJK DANK!

Meer informatie:

Ga naar **Dell.com/Endpoint-Security**



DELL Technologies