DELL Technologies

Saurez-vous vous montrer plus malin que votre cyberattaquant ?

Commencer

QUESTION 1 SUR 14

Hameçonnage

Vous recevez un e-mail de « Windows Defender Order » avec une facture de 399,99 $ qui semble officielle pour un abonnement d'un an à un compte Microsoft Defender. Il indique clairement « Veuillez ne pas répondre à cet e-mail », mais propose un bouton « Aide et contact » ainsi qu'un numéro de téléphone. Vous ne vous rappelez pas avoir commandé quelque chose de ce genre.

Que faites-vous ?

№ 1

Choisissez la réponse la mieux adaptée ci-dessous.

A Vous cliquez immédiatement sur le bouton « Aide et contact », car vous ne voulez surtout pas que votre carte de crédit soit débitée.

B Vous ouvrez l'e-mail dans une fenêtre incognito de votre navigateur Web et vous cliquez sur le bouton « Aide et contact ».

C Vous vérifiez votre relevé de carte de crédit en ligne pour voir si le débit a été effectué, puis vous utilisez le numéro de téléphone pour essayer d'obtenir davantage d'informations.

D Vous inspectez l'adresse e-mail et réalisez qu'elle semble louche. Vous cliquez donc sur le bouton « Signaler un hameçonnage » dans votre programme de messagerie et/ou vous le transmettez à votre département IT pour enquête (et, bien sûr, vous ne l'ouvrez pas !).

E Vous supprimez l'e-mail sans même l'ouvrir.

DELL Technologies

RÉPONSE

Hameçonnage

№ 1

BRAVO !

Signalez l’hameçonnage !

Lorsque vous recevez un e-mail suspect vous demandant de cliquer sur des liens pour quelque raison que ce soit, la meilleure chose à faire est de supprimer l’e-mail sans l’ouvrir ou de cliquer sur le bouton « Signaler un hameçonnage » dans votre barre d’outils Outlook afin de le signaler au département IT pour enquête. **Si ça semble louche, méfiez-vous.**

Question suivante

DELL Technologies

RÉPONSE

Hameçonnage

№ 1

BRAVO, MAIS...

Signalez l'hameçonnage !

Vous vous exposez tout de même à des risques en appelant ce qui sera probablement un faux numéro de téléphone. Mieux vaut opter pour l'une des autres solutions de cette liste. **Si ça semble louche, méfiez-vous.**

Question suivante

DELL Technologies

RÉPONSE

Hameçonnage

№ 1

PIRATAGE !

Signalez l’hameçonnage !

N’oubliez pas que lorsque vous recevez un e-mail suspect vous demandant de cliquer sur des liens pour quelque raison que ce soit, la meilleure chose à faire est de supprimer l’e-mail sans l’ouvrir ou de cliquer sur le bouton « Signaler un hameçonnage » dans votre barre d’outils Outlook afin de le signaler au département IT pour enquête. **Si ça semble louche, méfiez-vous.**

Question suivante

DELL Technologies

QUESTION 2 SUR 14

Hameçonnage sur les réseaux sociaux

Vous consultez votre compte Instagram et Lyle Lovett a répondu directement à votre commentaire sur sa publication. Il vous demande de le contacter directement par message et vous envoie un lien pour accéder à du contenu exclusif et intéressant d'un simple clic.

Vous :

№ 2

Choisissez la réponse la mieux adaptée ci-dessous.

A N'en revenez pas de votre chance et vous cliquez immédiatement sur le lien.

B Copiez le lien et l'ouvrez dans une fenêtre incognito.

C Partagez le lien avec vos amis sur les réseaux sociaux.

D Survolez le lien avec la souris et, comme vous suspectez qu'il y a quelque chose de louche, vous supprimez le message et bloquez l'expéditeur.

E Bloquez et signalez l'expéditeur sans cliquer sur quoi que ce soit.

DELL Technologies

RÉPONSE

Hameçonnage sur les réseaux sociaux

BRAVO !

Signalez l’hameçonnage !

Lorsque vous recevez un e-mail suspect vous demandant de cliquer sur des liens pour quelque raison que ce soit, la meilleure chose à faire est de supprimer l’e-mail sans l’ouvrir ou de cliquer sur le bouton « Signaler un hameçonnage » dans votre barre d’outils Outlook afin de le signaler au département IT pour enquête. **Si ça semble louche, méfiez-vous.**

Question suivante

DELL Technologies

RÉPONSE

Hameçonnage sur les réseaux sociaux

№ 2

PIRATAGE !

Signalez l’hameçonnage !

N’oubliez pas que lorsque vous recevez un e-mail suspect vous demandant de cliquer sur des liens pour quelque raison que ce soit, la meilleure chose à faire est de supprimer l’e-mail sans l’ouvrir ou de cliquer sur le bouton « Signaler un hameçonnage » dans votre barre d’outils Outlook afin de le signaler au département IT pour enquête. **Si ça semble louche, méfiez-vous.**

Question suivante

DELL Technologies

QUESTION 3 SUR 14

Sécurité des mots de passe

Votre département IT vous pousse à renforcer les mots de passe, parce que ces « informations d'identification » font partie des cibles de grande valeur que les attaquants recherchent. Donc...

Comment sécuriser davantage votre mot de passe ?

№ 3

Choisissez la réponse la mieux adaptée ci-dessous.

A Utilisez au moins 8 caractères, et de préférence davantage.

B Utilisez une combinaison de lettres, chiffres et caractères spéciaux.

C Évitez de réutiliser vos mots de passe pour des comptes ou des sites différents (utilisez un mot de passe unique pour chacun).

D Toutes les réponses qui précèdent.

E Aucune de ces réponses.

DELL Technologies

RÉPONSE

Sécurité des mots de passe

№ 3

BRAVO !

Utilisez un mot de passe fort.

Un mot de passe sécurisé est unique et combine au moins 8 lettres, chiffres et caractères spéciaux. Il peut même s'agir d'une phrase secrète dont vous vous souvenez. Et n'utilisez pas le nom de votre chien ! Assurez-vous également d'utiliser une authentification à deux facteurs. Combinée à un mot de passe fort, elle offre une protection optimale.

Question suivante

DELL Technologies

RÉPONSE

Sécurité des mots de passe

№ 3

BRAVO, MAIS...

Utilisez un mot de passe fort.

Un mot de passe sécurisé combine toutes les mesures de sécurité énumérées : il est unique et contient au moins 8 lettres, chiffres et caractères spéciaux. Et n'utilisez pas le nom de votre chien ! Pour plus de sécurité, utilisez l'authentification à deux facteurs et des phrases secrètes avec des chiffres et des caractères spéciaux au lieu de mots de passe.

Question suivante

DELL Technologies

RÉPONSE

Sécurité des mots de passe

№ 3

PIRATAGE !

Utilisez un mot de passe fort.

Un mot de passe sécurisé est unique et combine au moins 8 lettres, chiffres et caractères spéciaux. Pour plus de sécurité, utilisez l'authentification à deux facteurs et des phrases secrètes avec des chiffres et des caractères spéciaux au lieu de mots de passe.

Question suivante

DELL Technologies

QUESTION 4 SUR 14

Ingénierie sociale

Vous recevez un appel sur votre téléphone portable d'une personne qui dit faire partie de votre département IT vous informant que votre mot de passe a expiré et que vous devez en définir un nouveau. Le numéro de téléphone semble sûr. La personne vous demande de fournir votre numéro de collaborateur, votre numéro de sécurité sociale et votre date de naissance pour vérification.

Que faites-vous ?

Nº 4

Choisissez la réponse la mieux adaptée ci-dessous.

A Vous fournissez vos informations, car vous voulez réinitialiser votre mot de passe et vous remettre au travail.

B Vous demandez l'adresse e-mail et le numéro de téléphone de cette personne pour vérifier son identité, puis vous lui fournissez les informations qu'elle a demandées.

C Vous raccrochez immédiatement et signalez l'appel à votre département IT.

D Vous donnez votre numéro de collaborateur et votre date de naissance, mais pas votre numéro de sécurité sociale.

E Aucune de ces réponses.

DELL Technologies

RÉPONSE

Ingénierie sociale

№ 4

BRAVO !

Raccrochez et contactez le département IT.

Certains attaquants utilisent l'ingénierie sociale pour vous manipuler et vous amener à divulguer des données sensibles par téléphone. Même si vous êtes en mesure de vérifier dans votre système qu'il s'agit d'un collaborateur, il n'y a aucune garantie que vous soyez réellement en train de parler avec cette personne. **C'est vous qui devez toujours être à l'origine de vos réinitialisations de mot de passe.**

Question suivante

DELL Technologies

RÉPONSE

Ingénierie sociale

№ 4

PIRATAGE !

Raccrochez et contactez le département IT.

Certains attaquants utilisent l'ingénierie sociale pour vous manipuler et vous amener à divulguer des données sensibles par téléphone. Même si vous êtes en mesure de vérifier dans votre système qu'il s'agit d'un collaborateur, il n'y a aucune garantie que vous soyez réellement en train de parler avec cette personne. **C'est vous qui devez toujours être à l'origine de vos réinitialisations de mot de passe.**

Question suivante

DELL Technologies

QUESTION 5 SUR 14

Infiltration de PC

Pendant que vous êtes au téléphone, vous remarquez un comportement bizarre sur votre écran, comme la souris qui se déplace toute seule, des fenêtres de texte ou de console qui s'ouvrent et se ferment, ou des menus qui clignotent de haut en bas.

Donc :

Nº 5

Choisissez la réponse la mieux adaptée ci-dessous.

A Vous vous dites que c'est un problème de PC inoffensif et vous continuez à travailler.

B Vous en parlez à votre département IT, mais vous continuez à travailler.

C Vous cessez immédiatement d'utiliser votre PC, vous l'éteignez et vous contactez votre département IT (en utilisant un autre appareil) pour signaler le problème.

DELL Technologies

RÉPONSE

Infiltration de PC

№ 5

BRAVO !

Contactez immédiatement le département IT !

Le fait que votre souris se déplace « toute seule » sur l'écran peut être le signe d'une attaque sérieuse impliquant une violation de données et un éventuel enregistrement de frappe. Votre département IT doit en être informé le plus rapidement possible afin d'assurer un suivi efficace.

Question suivante

DELL Technologies

RÉPONSE

Infiltration de PC

№ 5

PIRATAGE !

Contactez immédiatement le département IT !

Un comportement anormal peut indiquer qu'un attaquant surveille votre PC, et pourrait à la fois exfiltrer des données et capturer des frappes au clavier, y compris vos mots de passe et autres informations stratégiques. Votre meilleure option consiste à éteindre immédiatement le PC et à signaler le problème à votre département IT.

Question suivante

DELL Technologies

QUESTION 6 SUR 14

Attaque de logiciels malveillants par USB

En traversant le parking de votre société, vous apercevez un sac déposé entre deux voitures. Vous remarquez qu'il contient cinq clés USB encore scellées dans leur emballage d'origine, de 500 Go chacune.

Que faites-vous ?

Nº 6

Choisissez la réponse la mieux adaptée ci-dessous.

A Vous en ouvrez une et l'insérez dans le port USB de votre PC, et vous donnez les quatre autres à vos collègues de travail.

B Vous les emportez chez vous et utilisez les clés USB sur votre ordinateur personnel.

C Vous informez le service de sécurité du bâtiment et votre département IT de la découverte et vous leur remettez les clés USB.

D Vous offrez les clés USB à vos enfants pour les fêtes.

E Aucune de ces réponses.

DELL Technologies

RÉPONSE

Attaque de logiciels malveillants par USB

Nº 6

BRAVO !

Informez les services de sécurité et le département IT.

Ce type d'attaque permet à un attaquant de placer un logiciel malveillant dans une organisation en utilisant un collaborateur comme « mule » pour l'insérer dans le réseau. N'insérez jamais une clé USB ou tout autre accessoire provenant d'une source inconnue dans un appareil que vous possédez, N'IMPORTE LEQUEL. Et par ailleurs, ce sont de très mauvais cadeaux.

Question suivante

DELL Technologies

RÉPONSE

Attaque de logiciels malveillants par USB

Nº 6

PIRATAGE !

Informez les services de sécurité et le département IT.

Ce type d'attaque permet à un attaquant de placer un logiciel malveillant dans une organisation en utilisant un collaborateur comme « mule » pour l'insérer dans le réseau. N'insérez jamais une clé USB ou tout autre accessoire provenant d'une source inconnue dans un appareil que vous possédez, N'IMPORTE LEQUEL. Et par ailleurs, ce sont de très mauvais cadeaux.

Question suivante

DELL Technologies

QUESTION 7 SUR 14

Rançongiciels

Un commercial se présente à votre bureau pour faire une présentation sur une nouvelle technologie que votre entreprise souhaite acquérir. Il apporte sa présentation sur une clé USB et vous demande de l'insérer dans votre PC afin qu'elle puisse être projetée pendant qu'il déroule son argumentaire.

Que faites-vous ?

N° 7

Choisissez la réponse la mieux adaptée ci-dessous.

A Vous faites ce qu'il vous demande et insérez la clé USB dans votre PC.

B Vous lui demandez si la présentation peut à la place être téléchargée, car la politique de votre société interdit l'utilisation de clés USB externes. Comme il ne peut pas la télécharger, vous faites ce qu'il demande et insérez la clé USB dans votre PC.

C Vous lui demandez d'effectuer la présentation sans projeter le support, et vous n'insérez pas la clé USB.

D Vous vous assurez qu'ils n'ont pas trouvé la clé USB dans un parking, puis vous l'insérez dans votre PC.

E Vous faites des copies supplémentaires de la clé USB et vous en donnez une à votre responsable.

DELL Technologies

RÉPONSE

Rançongiciels

№ 7

BRAVO !

Pas de projection, n’insérez pas la clé USB.

À votre insu, le commercial s’est vu offrir un gros pot-de-vin par un attaquant, et la clé USB contient un rançongiciel qui verrouillera vos systèmes. Mais si vous n’insérez pas la clé USB et ne téléchargez aucun autre fichier, vous empêchez l’attaquant d’obtenir l’accès à votre entreprise. Ouf.

Question suivante

DELL Technologies

RÉPONSE

Rançongiciels

№ 7

PIRATAGE !

Pas de projection, n’insérez pas la clé USB.

À votre insu, le commercial s’est vu offrir un gros pot-de-vin par un attaquant, et la clé USB ainsi que le fichier téléchargé contiennent un rançongiciel qui verrouillera vos systèmes. Évitez les clés USB externes et le téléchargement de fichiers de sources inconnues sur des PC personnels ou de votre société.

Question suivante

DELL Technologies

QUESTION 8 SUR 14

Authentification à deux facteurs

Votre banque vous a recommandé d'utiliser l'authentification à deux facteurs lorsque vous vous connectez à son site. D'autres sites Web utilisent également ce procédé pour assurer la sécurité des utilisateurs.

Parmi les options suivantes, laquelle est un exemple d'authentification à deux facteurs ?

№ 8

Choisissez la réponse la mieux adaptée ci-dessous.

A Vous saisissez votre nom d'utilisateur et votre mot de passe, puis vous êtes invité à entrer votre code PIN pour accéder au site Web.

B Vous saisissez votre nom d'utilisateur et votre mot de passe, ainsi qu'un CAPCHA où vous sélectionnez les images qui comprennent des panneaux.

C Vous saisissez votre nom d'utilisateur et votre mot de passe, et le site Web envoie un SMS sur votre téléphone portable avec un code à usage unique que vous saisissez dans la case prévue à cet effet sur le site Web.

D Vous saisissez votre nom d'utilisateur, et le site Web vous demande de saisir un code provenant d'un jeton sécurisé installé sur votre téléphone qui change chaque minute.

E A et C seulement.

F C et D seulement.

G Aucune de ces réponses.

DELL Technologies

RÉPONSE

Authentification à deux facteurs

BRAVO !

Il vous faut les deux.

L'authentification à deux facteurs requiert à la fois un mot de passe et un deuxième ID différent, par exemple un code envoyé par SMS ou un numéro généré par une application, pour identifier et authentifier les utilisateurs. Ce niveau de sécurité complique beaucoup l'accès à vos informations pour les attaquants.

Question suivante

DELL Technologies

RÉPONSE

Authentification à deux facteurs

BRAVO, MAIS...

Il vous faut les deux.

Vous y êtes presque. Il y a deux exemples d'authentification à deux facteurs ici. Réessayez et voyez si vous pouvez trouver l'autre.

Question suivante

DELL Technologies

RÉPONSE

Authentification à deux facteurs

PIRATAGE !

Oups. Il vous faut les deux.

L'authentification à deux facteurs requiert à la fois un mot de passe et un deuxième ID différent, par exemple un code envoyé par SMS ou un numéro généré par une application, pour identifier et authentifier les utilisateurs. Ce niveau de sécurité complique beaucoup l'accès à vos informations pour les attaquants. Si vous ne l'utilisez pas, vous êtes vulnérable aux attaques.

Question suivante

DELL Technologies

QUESTION 9 SUR 14

Voleurs par Bluetooth

Après avoir conduit jusqu'au départ d'un sentier pour commencer un bel après-midi de randonnée, vous réalisez que votre ordinateur portable est toujours dans votre sac à dos, et que vous avez votre téléphone avec vous (qui n'a pas de réseau). Vous devez laisser votre ordinateur et votre téléphone dans votre véhicule, mais vous voulez le faire de façon sécurisée.

Que faites-vous ?

№ 9

Choisissez la réponse la mieux adaptée ci-dessous.

A Vous désactivez entièrement le Wi-Fi.

B Vous placez votre ordinateur portable en mode veille.

C Vous verrouillez votre ordinateur portable et votre téléphone dans le coffre.

D Vous enveloppez votre ordinateur portable et votre téléphone dans une épaisse couverture.

E Vous éteignez complètement votre ordinateur portable et votre téléphone, ce qui désactive le Bluetooth.

DELL Technologies

RÉPONSE

Voleurs par Bluetooth

№ 9

BRAVO !

Éteignez votre ordinateur portable et votre téléphone.

Il est toujours préférable de dissimuler vos appareils lorsqu'ils sont sans surveillance, mais les voleurs utilisent des scanners Bluetooth pour localiser les appareils dans les véhicules verrouillés, et tous les appareils ne désactivent pas le Bluetooth lorsqu'ils sont « en veille ». Les vols se produisent souvent au départ des sentiers et à d'autres endroits où les propriétaires s'absentent pendant de longues périodes, et les voleurs sont toujours à l'affût. Donc, faites attention lorsque vous partez en randonnée.

Question suivante

DELL Technologies

RÉPONSE

Voleurs par Bluetooth

№ 9

PIRATAGE !

Éteignez votre ordinateur portable et votre téléphone.

Il est toujours préférable de dissimuler vos appareils lorsqu'ils sont sans surveillance, mais les voleurs utilisent des scanners Bluetooth pour localiser les appareils dans les véhicules verrouillés, et tous les appareils ne désactivent pas le Bluetooth lorsqu'ils sont « en veille ». Les vols se produisent souvent au départ des sentiers où les propriétaires seront absents pendant de longues périodes, donc faites attention lorsque vous partez en randonnée.

Question suivante

DELL Technologies

QUESTION 10 SUR 14

Attaque par USB - Partie 2

D’humeur festive, vous apportez un mini sapin de Noël alimenté par USB pour décorer votre bureau.

Comment l’alimentez-vous ?

№ 10

Choisissez la réponse la mieux adaptée ci-dessous.

A Vous le branchez sur votre PC.

B Vous le branchez sur une rallonge USB connectée à votre PC.

C Vous utilisez un chargeur USB dédié pour brancher l’appareil sur une prise de courant classique.

D Pas moyen de le brancher, il faut annuler Noël.

E Aucune de ces réponses.

DELL Technologies

RÉPONSE

Attaque par USB - Partie 2

№ 10

BRAVO !

Utilisez un chargeur USB dédié.

Cette variante d'attaque basée sur la technologie USB place des logiciels malveillants sur de nombreux appareils, même de petits sapins de Noël, ceci dans l'espoir qu'ils finissent par être branchés sur un précieux réseau d'entreprise. Ne connectez jamais un appareil USB inconnu à votre PC, même si c'est uniquement pour le charger.

Question suivante

DELL Technologies

RÉPONSE

Attaque par USB - Partie 2

№ 10

PIRATAGE !

Utilisez un chargeur USB dédié.

Cette variante d'attaque basée sur la technologie USB place des logiciels malveillants sur de nombreux appareils, même de petits sapins de Noël, ceci dans l'espoir qu'ils finissent par être branchés sur un précieux réseau d'entreprise. Ne connectez jamais un appareil USB inconnu à votre PC, même si c'est uniquement pour le charger.

Question suivante

DELL Technologies

QUESTION 11 SUR 14

Personnel malveillant

Vous participez à une conférence sur la cybersécurité à Shanghai, en Chine, et vous séjournez dans un hôtel 5 étoiles. Avant de sortir dîner, vous enfermez votre PC dans le coffre-fort de votre chambre.

Votre PC est-il en sécurité et protégé des attaques et du vol ?

№ 11

Choisissez la réponse la mieux adaptée ci-dessous.

A Non, car tout appareil laissé sans surveillance peut faire l'objet d'une attaque.

B Oui, car vous l'avez enfermé en toute sécurité dans le coffre.

C Oui, parce que vous avez aussi accroché des vêtements dans le placard pour dissimuler le coffre.

D Oui, parce que c'est un très bel hôtel.

E Oui, parce que ce n'est pas un très beau PC.

DELL Technologies

RÉPONSE

Personnel malveillant

№ 11

BRAVO !

Non, car tout appareil peut faire l’objet d’une attaque.

Tout appareil laissé sans surveillance peut être ouvert et compromis par ce qu’on désigne généralement comme l’attaque du « personnel malveillant », où un attaquant obtient l’accès en ouvrant physiquement le PC pour y insérer un logiciel malveillant. Un appareil qui n’est pas physiquement avec vous est vulnérable aux attaques. Par ailleurs, ne laissez jamais votre appareil aux mains d’un inconnu, car il peut s’agir de personnel malveillant.

Question suivante

DELL Technologies

RÉPONSE

Personnel malveillant

№ 11

PIRATAGE !

Non, car tout appareil peut faire l’objet d’une attaque.

Tout appareil laissé sans surveillance peut être ouvert et compromis par ce qu’on désigne généralement comme l’attaque du « personnel malveillant », où un attaquant obtient l’accès en ouvrant physiquement le PC pour y insérer un logiciel malveillant. Pour assurer leur sécurité, vous devez conserver vos appareils avec vous. Ne laissez jamais votre appareil aux mains d’un inconnu, car il peut s’agir de personnel malveillant.

Question suivante

DELL Technologies

QUESTION 12 SUR 14

Logiciels espions

Vous recevez un SMS d'un numéro vaguement familier qui vous annonce que votre fille a eu un accident et a été emmenée à l'hôpital. Il fournit un lien qui vous permet d'entrer en contact immédiatement.

Vous :

№ 12

Choisissez la réponse la mieux adaptée ci-dessous.

A Cliquez immédiatement sur le lien, parce que vous êtes inquiet pour votre fille.

B Faites une recherche sur le numéro, vous découvrez qu'il correspond à la région où se trouvait votre fille, puis vous cliquez sur le lien.

C Ne cliquez pas sur le lien, mais vous envoyez plutôt un message à votre fille pour vous assurer qu'elle va bien.

D Aucune de ces réponses.

DELL Technologies

RÉPONSE

Logiciels espions

№ 12

BRAVO !

Ne cliquez pas sur le lien.

Ce type d'attaque est une tentative de placer un logiciel espion sur votre téléphone, ce qui peut le compromettre et potentiellement se propager au réseau de l'entreprise. Vous avez identifié que cela ne semblait pas « normal » et avez utilisé une autre méthode pour vérifier que votre fille allait bien. Bien joué.

Question suivante

DELL Technologies

RÉPONSE

Logiciels espions

№ 12

PIRATAGE !

Ne cliquez pas sur le lien.

Ce type d'attaque est une tentative de placer un logiciel espion sur votre téléphone, ce qui peut le compromettre et potentiellement se propager au réseau de l'entreprise. Cliquer sur le lien entraîne le téléchargement d'un logiciel espion sur votre appareil. Rejetez en bloc les SMS étranges, peu importe ce qu'ils vous disent.

Question suivante

DELL Technologies

QUESTION 13 SUR 14

Sécurité des points de terminaison

Les acteurs de la menace (vous pourriez même les appeler des pirates ayant des intentions malveillantes) ciblent les points de terminaison.

Les points de terminaison sont définis comme suit :

№ 13

Choisissez la réponse la mieux adaptée ci-dessous.

A	Ordinateurs de bureau.
B	Ordinateurs portables et de bureau.
C	Ordinateurs de bureau, ordinateurs portables et serveurs.
D	Ordinateurs de bureau, ordinateurs portables, serveurs, Cloud et autres.
E	Ordinateurs portables et de bureau, serveurs, Cloud et dernière destination sur mon GPS.

DELL Technologies

RÉPONSE

Sécurité des points de terminaison

№ 13

BRAVO !

Tout appareil connecté distant.

Un point de terminaison est un dispositif connecté à distance à un réseau. La sécurité des points de terminaison est vitale pour protéger les appareils et les données de votre organisation, alors veillez à garder une longueur d'avance sur les attaquants.

Question suivante

DELL Technologies

RÉPONSE

Sécurité des points de terminaison

№ 13

BRAVO, MAIS...

Tout appareil connecté distant.

Un point de terminaison est un dispositif connecté à distance à un réseau. La sécurité des points de terminaison est vitale pour protéger les appareils et les données de votre organisation, alors veillez à garder une longueur d'avance sur les attaquants.

Question suivante

DELL Technologies

RÉPONSE

Sécurité des points de terminaison

№ 13

PIRATAGE !

Tout appareil connecté distant.

Un point de terminaison est un dispositif connecté à distance à un réseau. La sécurité des points de terminaison est vitale pour protéger les appareils et les données de votre organisation, alors veillez à garder une longueur d'avance sur les attaquants.

Question suivante

DELL Technologies

QUESTION 14 SUR 14

Sécurité des points de terminaison - Partie 2

Les pirates ayant des intentions malveillantes ciblent les points de terminaison comme les ordinateurs de bureau, les ordinateurs portables, les téléphones mobiles, les imprimantes sans fil, les serveurs, c'est-à-dire tout ce qui se connecte à un réseau.

Quelles mesures devez-vous prendre pour contribuer à empêcher une attaque ?

№ 14

Choisissez la réponse la mieux adaptée ci-dessous.

A M'assurer que je verrouille et que j'enferme mon appareil chaque fois que je ne l'utilise pas.

B Mettre à jour et appliquer les correctifs de mon appareil régulièrement.

C Avoir un bon comportement vis-à-vis des e-mails, en signalant ceux suspects.

D Ne jamais brancher un appareil inconnu sur mon point de terminaison.

E Toutes les réponses qui précèdent.

DELL Technologies

RÉPONSE

Sécurité des points de terminaison - Partie 2

№ 14

BRAVO !

Toutes les réponses ci-dessus.

Vous avez appris comment être cybersécurisé et vous mettez ces connaissances en pratique. La sécurité des points de terminaison est vitale pour protéger les appareils et les données de votre organisation, alors veillez à garder une longueur d'avance sur les attaquants.

Question suivante

DELL Technologies

RÉPONSE

Sécurité des points de terminaison - Partie 2

BRAVO, MAIS...

Il y a d’autres choses à faire.

Il y a plusieurs choses que vous devez faire pour protéger vos appareils. La sécurité des points de terminaison est vitale pour protéger les appareils et les données de votre organisation, alors veillez à garder une longueur d’avance sur les attaquants.

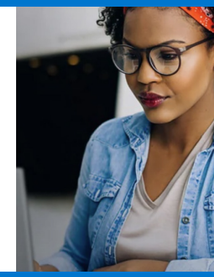
Question suivante

DELL Technologies

MERCI !

Pour en savoir plus :

Consultez **Dell.com/Endpoint-Security**



DELL Technologies