DELL Technologies

Sei un passo avanti rispetto ai criminali informatici?

Inizia il quiz

DOMANDA 1 DI 14

Phishing

Ricevi un'e-mail da "Windows Defender Order" contenente una fattura che sembra ufficiale di importo pari a $ 399,99 per un abbonamento annuale all'account Microsoft Defender. Riporta chiaramente il testo "Non rispondere a questa e-mail", ma contiene un pulsante "Assistenza e contatti" corredato da un numero di telefono. Tu non ricordi di avere ordinato nulla del genere.

Cosa fai?

1

Seleziona la risposta migliore di seguito

A Clicchi subito sul pulsante "Assistenza e contatti" per evitare l'addebito sulla tua carta di credito.

B Apri l'e-mail in una finestra in incognito del web browser e clicchi sul pulsante "Assistenza e contatti".

C Controlli l'estratto conto della carta di credito online per verificare se sia avvenuto l'addebito, quindi chiami il numero di telefono per provare a ottenere maggiori informazioni.

D Esamini l'indirizzo e-mail e ti rendi conto che sembra phishing, quindi clicchi su "Segnala phishing" nel programma di posta elettronica e/o inoltri l'e-mail al dipartimento IT per ulteriori indagini, e ovviamente non la apri.

E Elimini l'e-mail senza aprirla.

DELL Technologies

RISPOSTA

Phishing

1

BENE!

Segnala il phishing!

Se ricevi un'e-mail sospetta in cui ti si chiede di cliccare per qualsiasi motivo su un link, la soluzione migliore è eliminare l'e-mail senza aprirla oppure cliccare su "Segnala phishing" nella barra di Outlook per segnalarla al dipartimento IT che svolgerà ulteriori indagini. **Se sembra phishing, probabilmente lo è.**

Domanda successiva

DELL Technologies

RISPOSTA

Phishing

1

BENE, MA...

Segnala il phishing!

Se chiami un numero di telefono fasullo, ti esponi comunque a un rischio. Tra le opzioni c'è una soluzione migliore. **Se sembra phishing, probabilmente lo è.**

Domanda successiva

DELL Technologies

RISPOSTA

Phishing

1

ATTACCO IN CORSO!

Segnala il phishing!

Ricorda che, se ricevi un'e-mail sospetta in cui ti si chiede di cliccare per qualsiasi motivo su un link, la soluzione migliore è eliminare l'e-mail senza aprirla oppure cliccare su "Segnala phishing" nella barra di Outlook per segnalarla al dipartimento IT che svolgerà ulteriori indagini. **Se sembra phishing, probabilmente lo è.**

Domanda successiva

DELL Technologies

DOMANDA 2 DI 14

Phishing sui social media

Mentre controlli il tuo account Instagram, ti accorgi che Lyle Lovett ha risposto direttamente a un tuo commento sotto il suo post. Ti chiede di metterti in contatto con lui con un messaggio diretto e ti invia un link su cui cliccare per accedere a contenuti importanti e riservati a pochi.

Tu:

2

Seleziona la risposta migliore di seguito

A Non riesci a credere ai tuoi occhi e clicchi subito sul link.

B Copi il link e lo apri in una finestra in incognito.

C Condividi il link con i tuoi amici sui social media.

D Passi il mouse sul link e sospetti che si tratti di phishing, quindi elimini il messaggio e blocchi il mittente.

E Blocchi e segnali il mittente senza cliccare su nulla.

DELL Technologies

RISPOSTA

Phishing sui social media

BENE!

Segnala il phishing!

Se ricevi un'e-mail sospetta in cui ti si chiede di cliccare per qualsiasi motivo su un link, la soluzione migliore è eliminare l'e-mail senza aprirla oppure cliccare su "Segnala phishing" nella barra di Outlook per segnalarla al dipartimento IT che svolgerà ulteriori indagini. **Se sembra phishing, probabilmente lo è.**

Domanda successiva

DELL Technologies

RISPOSTA

Phishing sui social media

ATTACCO IN CORSO!

Segnala il phishing!

Ricorda che, se ricevi un'e-mail sospetta in cui ti si chiede di cliccare per qualsiasi motivo su un link, la soluzione migliore è eliminare l'e-mail senza aprirla oppure cliccare su "Segnala phishing" nella barra di Outlook per segnalarla al dipartimento IT che svolgerà ulteriori indagini. **Se sembra phishing, probabilmente lo è.**

Domanda successiva

DELL Technologies

DOMANDA 3 DI 14

Sicurezza delle password

Il dipartimento IT ti spinge ad aumentare la complessità delle password, poiché queste "credenziali" sono tra gli obiettivi di maggior valore per i malintenzionati. Quindi...

Come fai a incrementare la sicurezza della password?

3

Seleziona la risposta migliore di seguito

A	Ne scegli una di almeno 8 caratteri, preferibilmente di più.
B	Utilizzi una combinazione di lettere, numeri e simboli.
C	Eviti di riutilizzare la stessa password su più account o siti (fai in modo che ognuna sia univoca).
D	Tutte le risposte precedenti.
E	Nessuna delle risposte precedenti.

DELL Technologies

RISPOSTA

Sicurezza delle password

BENE!

Utilizza una password complessa!

Una password è considerata sicura quando è univoca e costituita da almeno 8 lettere, numeri e simboli e magari utilizza una passphrase univoca che ricordi. Evita di utilizzare il nome del tuo cane! Inoltre, ricorda di utilizzare l'autenticazione a due fattori che, insieme a una password complessa, offre livelli di protezione ottimali.

Domanda successiva

DELL Technologies

RISPOSTA

Sicurezza delle password

BENE, MA...

Utilizza una password complessa!

Una password sicura combina tutte le misure di sicurezza indicate: è univoca e contiene almeno 8 lettere, numeri e simboli. Evita di utilizzare il nome del tuo cane! Per una maggiore sicurezza, utilizza l'autenticazione a due fattori e le passphrase con numeri e simboli, anziché le password.

Domanda successiva

DELL Technologies

RISPOSTA

Sicurezza delle password

ATTACCO IN CORSO!

Utilizza una password complessa!

Una password sicura è univoca e contiene almeno 8 lettere, numeri e simboli. Per una maggiore sicurezza, utilizza l'autenticazione a due fattori e le passphrase con numeri e simboli, anziché le password.

Domanda successiva

DELL Technologies

DOMANDA 4 DI 14

Social engineering

Ti chiama sul cellulare una persona che sostiene di lavorare per il dipartimento IT della tua azienda, la quale ti informa che la tua password è scaduta e che bisogna impostarne una nuova. Il numero di telefono sembra sicuro. Ti chiede quindi di comunicarle il tuo numero dipendente, il tuo numero di previdenza sociale e la tua data di nascita per una verifica.

Cosa fai?

4

Seleziona la risposta migliore di seguito

A Le fornisci le informazioni richieste, in modo da ripristinare la password e rimetterti al lavoro.

B Le chiedi il suo indirizzo e-mail e numero di telefono per verificarne l'identità, quindi le fornisci le informazioni richieste.

C Interrompi immediatamente la chiamata ed effettui una segnalazione al dipartimento IT.

D Le fornisci il numero dipendente e la data di nascita, ma tieni per te il numero di previdenza sociale.

E Nessuna delle risposte precedenti.

DELL Technologies

RISPOSTA

Social engineering

4

BENE!

Stacca e contatta il team IT!

Alcuni malintenzionati utilizzano il social engineering per manipolarti e spingerti a fornire telefonicamente informazioni sensibili. Anche se riesci a verificare che si tratta di un dipendente presente nel sistema, non hai garanzie che dall'altro capo del telefono ci sia realmente la persona in questione. **È importante intraprendere sempre in autonomia il ripristino delle proprie password.**

Domanda successiva

DELL Technologies

RISPOSTA

Social engineering

4

ATTACCO IN CORSO!

Stacca e contatta il team IT!

Alcuni malintenzionati utilizzano il social engineering per manipolarti e spingerti a fornire telefonicamente informazioni sensibili. Anche se riesci a verificare che si tratta di un dipendente presente nel sistema, non hai garanzie che dall'altro capo del telefono ci sia realmente la persona in questione. **È importante intraprendere sempre in autonomia il ripristino delle proprie password.**

Domanda successiva

DELL Technologies

DOMANDA 5 DI 14

Infiltrazioni nel PC

Sei al telefono e noti alcuni comportamenti strani sullo schermo del PC, come il cursore che si muove da solo, finestre della console o di testo che si aprono e si chiudono o menu che lampeggiano.

A questo punto:

5

Seleziona la risposta migliore di seguito

A Immagini che sia un problema innocuo del PC e continui a lavorare.

B Chiedi delucidazioni al dipartimento IT, ma continui a lavorare.

C Smetti immediatamente di utilizzare il PC, lo arresti e segnali il problema al dipartimento IT (con un altro dispositivo).

DELL Technologies

RISPOSTA

Infiltrazioni nel PC

5

BENE!

Contatta subito il team IT!

Talvolta il cursore che si muove "da solo" sullo schermo è sintomo di un grave attacco che implica una violazione dei dati e un possibile key logging. Occorre informarne al più presto il dipartimento IT, il quale darà efficacemente seguito alla questione.

Domanda successiva

DELL Technologies

RISPOSTA

Infiltrazioni nel PC

5

ATTACCO IN CORSO!

Contatta subito il team IT!

Talvolta un comportamento anomalo indica che un malintenzionato sta monitorando il PC e potrebbe sottrarre dati e registrare le digitazioni, incluse le password e altre informazioni cruciali. La soluzione migliore è arrestare subito il PC e segnalare il problema al dipartimento IT.

Domanda successiva

DELL Technologies

DOMANDA 6 DI 14

Attacco malware tramite USB

Cammini nel parcheggio della tua azienda e scorgi un sacchetto a terra tra due auto. Al suo interno trovi cinque unità USB da 500 GB ciascuna, ancora sigillate nella confezione originale.

Cosa fai?

6

Seleziona la risposta migliore di seguito

A Ne apri una e la inserisci nello slot USB del tuo PC e dai le altre quattro ai tuoi colleghi.

B Porti le unità USB a casa e le utilizzi sul tuo personal computer.

C Informi la sicurezza dell'edificio e il dipartimento IT del ritrovamento e consegni loro le unità USB.

D Regali le unità USB ai tuoi figli per Natale.

E Nessuna delle risposte precedenti.

DELL Technologies

RISPOSTA

Attacco malware tramite USB

BENE!

Informa la sicurezza e il team IT!

In questo tipo di attacco, il malintenzionato introduce il malware all'interno dell'organizzazione utilizzando un dipendente come "corriere" per inserire il payload malevolo nella rete. Non inserire mai un'unità USB o altri accessori di origine sconosciuta in NESSUNO dei dispositivi che utilizzi. E sono davvero pessimi regali!

Domanda successiva

DELL Technologies

RISPOSTA

Attacco malware tramite USB

6

ATTACCO IN CORSO!

Informa la sicurezza e il team IT!

In questo tipo di attacco, il malintenzionato introduce il malware all'interno dell'organizzazione utilizzando un dipendente come "corriere" per inserire il payload malevolo nella rete. Non inserire mai un'unità USB o altri accessori di origine sconosciuta in NESSUNO dei dispositivi che utilizzi. E sono davvero pessimi regali!

Domanda successiva

DELL Technologies

DOMANDA 7 DI 14

Ransomware

Ricevi in ufficio un rappresentante intenzionato a presentare alcune nuove tecnologie che la tua azienda è interessata ad acquisire. La presentazione si trova su un'unità USB, che ti chiede di inserire nel tuo PC, in modo da proiettarla durante il discorso.

Cosa fai?

7

Seleziona la risposta migliore di seguito

A Fai ciò che ti chiede e inserisci l'unità USB nel tuo PC.

B Gli chiedi se sia possibile scaricare la presentazione, dal momento che la policy aziendale proibisce l'utilizzo di unità USB esterne. Non essendo possibile, fai ciò che ti chiede e inserisci l'unità USB nel tuo PC.

C Gli chiedi di effettuare la presentazione senza proiettarla e non inserisci l'unità USB.

D Ti accerti che non abbia trovato l'unità USB in un parcheggio, quindi la inserisci nel tuo PC.

E Effettui altre copie dell'unità USB e ne consegni una al tuo responsabile.

DELL Technologies

RISPOSTA

Ransomware

7

BENE!

Non acconsentire alla proiezione e non inserire l'unità USB.

A tua insaputa, un malintenzionato ha offerto al rappresentante un'ingente somma di denaro e l'unità USB contiene un payload ransomware che bloccherà i sistemi. Non collegandola e non scaricando nessun altro file, impedisci l'accesso al malintenzionato. Sensazionale!

Domanda successiva

DELL Technologies

RISPOSTA

Ransomware

7

ATTACCO IN CORSO!

Non acconsentire alla proiezione e non inserire l'unità USB.

A tua insaputa, un malintenzionato ha offerto al rappresentante un'ingente somma di denaro e l'unità USB e il file scaricato contengono un payload ransomware che bloccherà i sistemi. Evita di inserire unità USB esterne e di scaricare file da fonti sconosciute su PC personali o aziendali.

Domanda successiva

DELL Technologies

DOMANDA 8 DI 14

Autenticazione a due fattori

La tua banca ti ha consigliato di utilizzare l'autenticazione a due fattori per accedere al suo sito. Anche altri siti web utilizzano questa procedura per la sicurezza degli utenti.

Quale delle seguenti opzioni è un esempio di autenticazione a due fattori?

8

Seleziona la risposta migliore di seguito

A	Inserire prima nome utente e password e poi il proprio PIN per accedere al sito web.
B	Inserire prima nome utente e password e poi un CAPCHA da cui selezionare le immagini su cui sono raffigurati cartelli.
C	Inserire prima nome utente e password, poi si riceve sul cellulare un SMS contenente un codice monouso da inserire nella casella presente sul sito web.
D	Inserire prima il nome utente, poi il sito web chiede di inserire un codice da un token protetto che cambia ogni minuto ed è installato sul telefono.
E	Soltanto A e C.
F	Soltanto C e D.
G	Nessuna delle risposte precedenti.

DELL Technologies

RISPOSTA

Autenticazione a due fattori

BENE!

Servono entrambi!

L'autenticazione a due fattori richiede una password e un secondo e diverso metodo di identificazione, come un codice inviato tramite SMS o un numero generato da un'app, per identificare e autenticare gli utenti. Questo livello di sicurezza complica l'accesso dei malintenzionati alle tue informazioni.

Domanda successiva

DELL Technologies

RISPOSTA

Autenticazione a due fattori

BENE, MA...

Servono entrambi!

Ci sei quasi! Sono presenti due esempi di autenticazione a due fattori. Ritenta e prova a individuare l'altro.

Domanda successiva

DELL Technologies

RISPOSTA

Autenticazione a due fattori

ATTACCO IN CORSO!

Ops! Servono entrambi!

L'autenticazione a due fattori richiede una password e un secondo e diverso metodo di identificazione, come un codice inviato tramite SMS o un numero generato da un'app, per identificare e autenticare gli utenti. Questo livello di sicurezza complica l'accesso dei malintenzionati alle tue informazioni. Se non te ne avvali, rimani vulnerabile agli attacchi dei malintenzionati.

Domanda successiva

DELL Technologies

DOMANDA 9 DI 14

Furti tramite Bluetooth

Ti trovi all'inizio di un sentiero per un bel pomeriggio di trekking quando ti rendi conto di avere ancora il notebook nello zaino e il cellulare (che non ha campo) con te. Hai bisogno di lasciare il computer e il telefono in auto, ma occorre proteggerli.

Cosa fai?

9

Seleziona la risposta migliore di seguito

A Disattivi il Wi-Fi.

B Metti il notebook in modalità di sospensione.

C Chiudi il notebook e il telefono nel bagagliaio.

D Avvolgi il notebook e il telefono in una coperta spessa.

E Spegni completamente il notebook e il telefono, disattivando così anche il Bluetooth.

DELL Technologies

RISPOSTA

Furti tramite Bluetooth

BENE!

Spegni il notebook e il telefono!

È sempre buona norma tenere lontani da occhi indiscreti i dispositivi lasciati incustoditi, ma i ladri utilizzano scanner Bluetooth per individuare i dispositivi nei veicoli chiusi e non per tutti l'attivazione della modalità di sospensione comporta la disattivazione del Bluetooth. I furti si verificano spesso in prossimità di sentieri e in altri luoghi in cui i proprietari restano lontani per lunghi periodi; i ladri sono sempre in agguato! Ricordalo prima della tua prossima escursione.

Domanda successiva

DELL Technologies

RISPOSTA

Furti tramite Bluetooth

ATTACCO IN CORSO!

Spegni il notebook e il telefono!

È sempre buona norma tenere lontani da occhi indiscreti i dispositivi lasciati incustoditi, ma i ladri utilizzano scanner Bluetooth per individuare i dispositivi nei veicoli chiusi e non per tutti l'attivazione della modalità di sospensione comporta la disattivazione del Bluetooth. I furti si verificano spesso in prossimità di sentieri dove i proprietari restano lontani per lunghi periodi; ricordalo prima della tua prossima escursione.

Domanda successiva

DELL Technologies

DOMANDA 10 DI 14

Attacco tramite USB (parte 2)

Sei in vena di festa e porti in ufficio un mini albero di Natale con cavo USB.

Come lo alimenti?

10

Seleziona la risposta migliore di seguito

A Lo colleghi al tuo PC.

B Lo colleghi a un extender USB collegato al tuo PC.

C Utilizzi un caricabatterie USB dedicato per collegare il dispositivo alla presa di corrente standard.

D Non c'è modo di alimentarlo, il Natale è bandito.

E Nessuna delle risposte precedenti.

DELL Technologies

RISPOSTA

Attacco tramite USB (parte 2)

10

BENE!

Utilizza un caricabatterie USB dedicato!

Questa variante di attacco tramite USB prevede l'inserimento di malware all'interno dei dispositivi più disparati, persino nei mini alberi di Natale, nella speranza che qualcuno li colleghi in una rete aziendale ricca di possibilità. Non collegare mai un dispositivo USB sconosciuto al tuo PC, nemmeno per ricaricarlo.

Domanda successiva

DELL Technologies

RISPOSTA

Attacco tramite USB (parte 2)

10

ATTACCO IN CORSO!

Utilizza un caricabatterie USB dedicato!

Questa variante di attacco tramite USB prevede l'inserimento di malware all'interno dei dispositivi più disparati, persino nei mini alberi di Natale, nella speranza che qualcuno li colleghi in una rete aziendale ricca di possibilità. Non collegare mai un dispositivo USB sconosciuto al tuo PC, nemmeno per ricaricarlo.

Domanda successiva

DELL Technologies

DOMANDA 11 DI 14

Evil Maid

Ti trovi a Shanghai, in Cina, per una conferenza sulla sicurezza informatica e soggiorni in un hotel a cinque stelle. Prima di uscire per cena, chiudi il PC nella cassaforte della tua stanza.

Il PC è al sicuro da attacchi e furti?

11

Seleziona la risposta migliore di seguito

A	No, perché qualsiasi dispositivo lasciato incustodito può essere oggetto di violazioni.
B	Sì, perché l'hai chiuso in sicurezza nella cassaforte.
C	Sì, perché nell'armadio hai anche appeso degli indumenti che nascondono la cassaforte.
D	Sì, perché è davvero un ottimo hotel.
E	Sì, perché non è un granché come PC.

DELL Technologies

RISPOSTA

Evil Maid

11

BENE!

No, qualsiasi dispositivo può essere oggetto di violazioni!

Qualsiasi dispositivo lasciato incustodito può essere aperto e compromesso tramite un attacco comunemente detto "Evil Maid" (cameriera malvagia), nel quale il malintenzionato ottiene l'accesso con l'apertura materiale del PC per inserirvi il malware. Sono esposti all'attacco tutti i dispositivi che non porti fisicamente con te. Inoltre, non lasciare mai il tuo dispositivo a uno sconosciuto, tanto meno a un'evil maid.

Domanda successiva

DELL Technologies

RISPOSTA

Evil Maid

11

ATTACCO IN CORSO!

No, qualsiasi dispositivo può essere oggetto di violazioni!

Qualsiasi dispositivo lasciato incustodito può essere aperto e compromesso tramite un attacco comunemente definito "Evil Maid" (cameriera malvagia), nel quale il malintenzionato ottiene l'accesso con l'apertura materiale del PC per inserirvi il malware. Per a massima sicurezza, porta sempre con te tutti i tuoi dispositivi. Non lasciarli a uno sconosciuto, tanto meno a un'evil maid.

Domanda successiva

DELL Technologies

DOMANDA 12 DI 14

Spyware

Ricevi un SMS da un numero vagamente familiare, il quale ti informa che tua figlia ha avuto un incidente ed è stata portata in ospedale. Contiene anche un link per metterti subito in contatto con i sanitari.

Tu:

12

Seleziona la risposta migliore di seguito

A	Clicchi subito sul link perché temi per la salute di tua figlia.
B	Fai una ricerca sul numero, scopri che è della zona in cui si trovava tua figlia e clicchi sul link.
C	Non clicchi sul link e mandi un messaggio a tua figlia per accertarti che stia bene.
D	Nessuna delle risposte precedenti.

DELL Technologies

RISPOSTA

Spyware

12

BENE!

Non cliccare sul link!

Questo tipo di attacco è un tentativo di inserire spyware sul tuo telefono, al fine di comprometterlo e potenzialmente diffondere lo spyware sulla rete aziendale. Il messaggio non ti è sembrato "autentico" e hai utilizzato un altro metodo per verificare che tua figlia stesse bene. Ben fatto!

Domanda successiva

DELL Technologies

RISPOSTA

Spyware

12

ATTACCO IN CORSO!

Non cliccare sul link!

Questo tipo di attacco è un tentativo di inserire spyware sul tuo telefono, al fine di comprometterlo e potenzialmente diffondere lo spyware sulla rete aziendale. Se clicchi sul link, introduci un payload spyware sul tuo dispositivo. Di' no ai messaggi vaghi, indipendentemente da quanto sembrino persuasivi.

Domanda successiva

DELL Technologies

DOMANDA 13 DI 14

Sicurezza degli endpoint

I malintenzionati (puoi anche chiamarli hacker con intenzioni malevole) puntano agli endpoint.

Gli endpoint sono:

13

Seleziona la risposta migliore di seguito

A Desktop.

B Desktop e notebook.

C Desktop, notebook e server.

D Desktop, notebook, server, cloud e altro.

E Desktop, notebook, server, cloud e l'ultima destinazione del mio GPS.

DELL Technologies

RISPOSTA

13

Sicurezza degli endpoint

BENE!

Qualsiasi dispositivo connesso da remoto!

Un endpoint è costituito da qualsiasi dispositivo connesso da remoto a una rete. La sicurezza degli endpoint è fondamentale per proteggere i dispositivi e i dati della tua organizzazione; resta sempre un passo avanti rispetto ai malintenzionati.

Domanda successiva

DELL Technologies

RISPOSTA

Sicurezza degli endpoint

13

BENE, MA...

Qualsiasi dispositivo connesso da remoto!

Un endpoint è costituito da qualsiasi dispositivo connesso da remoto a una rete. La sicurezza degli endpoint è fondamentale per proteggere i dispositivi e i dati della tua organizzazione; resta sempre un passo avanti rispetto ai malintenzionati.

Domanda successiva

DELL Technologies

RISPOSTA

13

Sicurezza degli endpoint

ATTACCO IN CORSO!

Qualsiasi dispositivo connesso da remoto!

Un endpoint è costituito da qualsiasi dispositivo connesso da remoto a una rete. La sicurezza degli endpoint è fondamentale per proteggere i dispositivi e i dati della tua organizzazione; resta sempre un passo avanti rispetto ai malintenzionati.

Domanda successiva

DELL Technologies

DOMANDA 14 DI 14

Sicurezza degli endpoint (parte 2)

Gli hacker con intenti malevoli puntano agli endpoint, quali desktop, notebook, telefoni cellulari, stampanti senza fili, server, insomma qualsiasi dispositivo connesso a una rete.

Cosa bisognerebbe fare per prevenire un attacco?

14

Seleziona la risposta migliore di seguito

A	Accertarsi di bloccare e chiudere a chiave il dispositivo quando non è in uso.
B	Aggiornare e applicare regolarmente le patch sul dispositivo.
C	Adottare una corretta igiene delle e-mail: segnalare le e-mail sospette.
D	Non collegare mai un dispositivo sconosciuto al proprio endpoint.
E	Tutte le risposte precedenti.

DELL Technologies

RISPOSTA

Sicurezza degli endpoint (parte 2)

BENE!

Tutte le risposte precedenti!

Hai imparato come salvaguardare la sicurezza informatica e lo stai mettendo in pratica. La sicurezza degli endpoint è fondamentale per proteggere i dispositivi e i dati della tua organizzazione; resta sempre un passo avanti rispetto ai malintenzionati.

Domanda successiva

DELL Technologies

RISPOSTA

Sicurezza degli endpoint (parte 2)

BENE, MA...

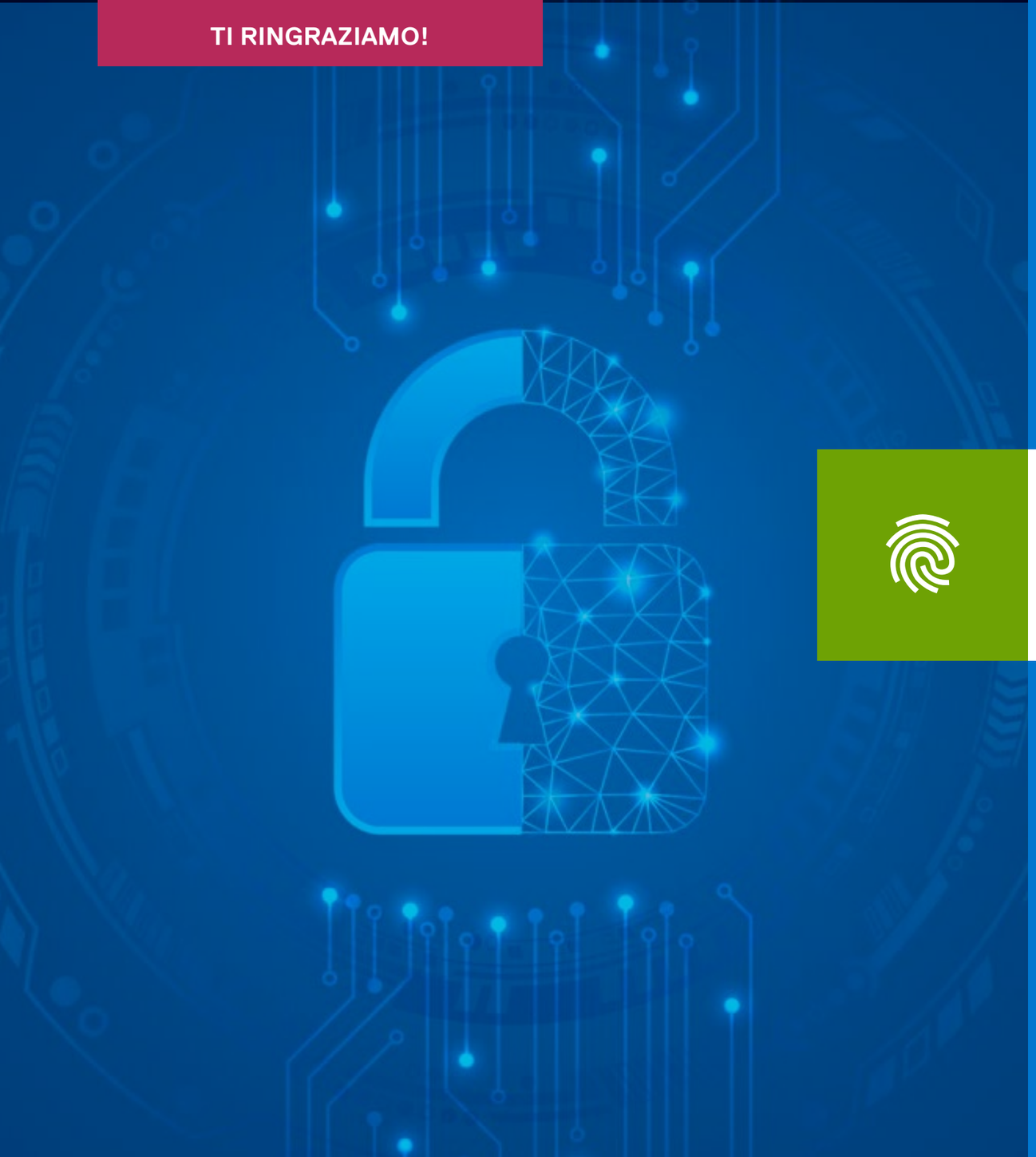
C'è di più!

Ci sono altre misure da adottare per proteggere i dispositivi. La sicurezza degli endpoint è fondamentale per proteggere i dispositivi e i dati della tua organizzazione; resta sempre un passo avanti rispetto ai malintenzionati.

Domanda successiva

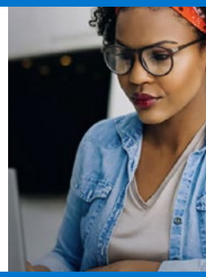
DELL Technologies

TI RINGRAZIAMO!



Per ulteriori informazioni:

visita il sito **Dell.com/Endpoint-Security**



DELL Technologies