DELL Technologies

Sind Sie schlauer als Cyberkriminelle?

Quiz starten

FRAGE 1 VON 14

Phishing

Sie erhalten eine E-Mail von „Windows Defender Order“ mit einer Rechnung über 399,99 US-Dollar für ein 1-Jahres-Abonnement für ein Microsoft Defender-Konto. Das Dokument sieht nach einer offiziellen Rechnung aus. In der E-Mail ist klar angegeben, dass nicht auf die E-Mail geantwortet werden soll, aber sie enthält eine Schaltfläche „Hilfe und Kontakt“ sowie eine Telefonnummer. Sie können sich nicht erinnern, etwas in dieser Art bestellt zu haben.

Was tun Sie?

Nr. 1

Wählen Sie unten die beste Antwort aus.

A Sie klicken sofort auf die Schaltfläche „Hilfe und Kontakt“, denn diese Gebühr soll definitiv nicht über Ihre Kreditkarte abgebucht werden.

B Sie öffnen die E-Mail in einem Inkognitofenster Ihres Webbrowsers und klicken auf die Schaltfläche „Hilfe und Kontakt“.

C Sie überprüfen Ihre Kreditkartenabrechnung online, um zu sehen, ob die Gebühr abgebucht wurde, und versuchen dann mithilfe der Telefonnummer, mehr über die Sache zu erfahren.

D Sie sehen sich die E-Mail-Adresse genau an und empfinden sie als suspekt, also klicken Sie in Ihrem E-Mail-Programm auf „Phishing melden“ und/oder leiten die E-Mail zur Überprüfung an Ihre IT-Abteilung weiter – natürlich ohne die E-Mail zu öffnen!

E Sie löschen die E-Mail, ohne sie zu öffnen.

DELL Technologies

ANTWORT

Phishing

Nr. 1

GUT GEMACHT!

Phishing melden!

Wenn Sie eine verdächtige E-Mail erhalten, in der Sie aus irgendeinem Grund auf Links klicken sollen, sollten Sie die E-Mail löschen, ohne sie zu öffnen, oder in Ihrem Outlook auf „Phishing melden“ klicken, um die E-Mail zur Überprüfung bei der IT zu melden. **Wenn etwas nach Phishing aussieht, ist es das wahrscheinlich auch.**

Nächste Frage

DELL Technologies

ANTWORT

Phishing

Nr. 1

GUT GEMACHT, ABER ...

Phishing melden!

Wenn Sie eine Nummer anrufen, die sich als gefälscht herausstellt, setzen Sie sich Risiken aus. Eine andere Option aus der Liste wäre eine bessere Lösung.

Wenn etwas nach Phishing aussieht, ist es das wahrscheinlich auch.

Nächste Frage

DELL Technologies

ANTWORT

Phishing

Nr. 1

GEHACKT!!!

Phishing melden!

Nicht vergessen: Wenn Sie eine verdächtige E-Mail erhalten, in der Sie aus irgendeinem Grund auf Links klicken sollen, sollten Sie die E-Mail löschen, ohne sie zu öffnen, oder in Ihrem E-Mail-Programm auf „Phishing melden“ klicken, um die E-Mail zur Überprüfung bei der IT zu melden. **Wenn etwas nach Phishing aussieht, ist es das wahrscheinlich auch.**

Nächste Frage

DELL Technologies

FRAGE 2 VON 14

Social-Media-Phishing

Sie sehen sich Ihren Instagram-Account an und Lyle Lovett hat direkt auf Ihren Kommentar zu seinen Posts geantwortet. Er bittet Sie, sich per Direktnachricht mit ihm in Verbindung zu setzen, und sendet Ihnen einen Link zu stark limitierten und wertvollen Inhalten.

Was tun Sie?

Nr. 2

Wählen Sie unten die beste Antwort aus.

A Sie können Ihr Glück kaum fassen und klicken sofort auf den Link.

B Sie kopieren den Link und öffnen ihn in einem Inkognitofenster.

C Sie teilen den Link auf Social Media mit Ihren FreundInnen.

D Sie ziehen die Maus über den Link und vermuten, dass an der Sache etwas faul ist. Also löschen Sie die Nachricht und sperren den Sender.

E Sie sperren und melden den Sender, ohne auf irgendetwas zu klicken.

DELL Technologies

ANTWORT

Social-Media-Phishing

Nr. 2

GUT GEMACHT!

Phishing melden!

Wenn Sie eine verdächtige E-Mail erhalten, in der Sie aus irgendeinem Grund auf Links klicken sollen, sollten Sie die E-Mail löschen, ohne sie zu öffnen, oder in Ihrem Outlook auf „Phishing melden“ klicken, um die E-Mail zur Überprüfung bei der IT zu melden. **Wenn etwas nach Phishing aussieht, ist es das wahrscheinlich auch.**

Nächste Frage

DELL Technologies

ANTWORT

Social-Media-Phishing

Nr. 2

GEHACKT!!!

Phishing melden!

Nicht vergessen: Wenn Sie eine verdächtige E-Mail erhalten, in der Sie aus irgendeinem Grund auf Links klicken sollen, sollten Sie die E-Mail löschen, ohne sie zu öffnen, oder in Ihrem E-Mail-Programm auf „Phishing melden“ klicken, um die E-Mail zur Überprüfung bei der IT zu melden. **Wenn etwas nach Phishing aussieht, ist es das wahrscheinlich auch.**

Nächste Frage

DELL Technologies

FRAGE 3 VON 14

Kennwortsicherheit

Ihre IT-Abteilung pocht auf sichere Kennwörter, weil Zugangsdaten zu den wertvollsten Zielen von Angreifern gehören. Also ...

Wie können Sie Ihr Kennwort sicherer machen?

Nr. 3

Wählen Sie unten die beste Antwort aus.

A Sie achten darauf, dass es mindestens 8 Zeichen lang ist, am besten noch länger.

B Sie verwenden eine Kombination aus Buchstaben, Ziffern und Zeichen.

C Sie nutzen für verschiedene Konten oder Websites nicht dasselbe, sondern immer ein anderes Kennwort.

D Alle oben genannten Antworten.

E Keine der oben genannten Antworten.

DELL Technologies

ANTWORT

Kennwortsicherheit

Nr. 3

GUT GEMACHT!

Ein sicheres Kennwort verwenden!

Ein sicheres Kennwort ist einzigartig und kombiniert mindestens 8 Buchstaben, Ziffern und Zeichen. Vielleicht verwenden Sie sogar eine individuelle Passphrase, an die Sie sich erinnern. Und verwenden Sie nicht den Namen Ihres Hundes! Außerdem sollten Sie die Zwei-Faktor-Authentifizierung nutzen. Zusammen mit einem sicheren Kennwort wird so für optimalen Schutz gesorgt.

Nächste Frage

DELL Technologies

ANTWORT

Kennwortsicherheit

Nr. 3

GUT GEMACHT, ABER ...

Ein sicheres Kennwort verwenden!

Ein sicheres Kennwort kombiniert alle genannten Sicherheitsmaßnahmen: Es ist einzigartig und besteht aus mindestens 8 Buchstaben, Ziffern und Zeichen. Und verwenden Sie nicht den Namen Ihres Hundes! Für zusätzliche Sicherheit sollten Sie die Zwei-Faktor-Authentifizierung und Passphrasen mit Ziffern und Zeichen anstelle von Kennwörtern nutzen.

Nächste Frage

DELL Technologies

ANTWORT

Kennwortsicherheit

Nr. 3

GEHACKT!!!

Ein sicheres Kennwort verwenden!

Ein sicheres Kennwort ist einzigartig und kombiniert mindestens 8 Buchstaben, Ziffern und Zeichen. Für zusätzliche Sicherheit sollten Sie die Zwei-Faktor-Authentifizierung und Passphrasen mit Ziffern und Zeichen anstelle von Kennwörtern nutzen.

Nächste Frage

DELL Technologies

FRAGE 4 VON 14

Social Engineering

Auf Ihrem Mobiltelefon geht ein Anruf einer Person ein, die behauptet, zu Ihrer IT-Abteilung zu gehören. Die Person sagt Ihnen, dass Ihr Kennwort abgelaufen ist und Sie ein neues einrichten müssen. Die Telefonnummer sieht sicher aus. Die Person bittet Sie, zwecks Verifizierung Ihre Mitarbeiternummer, Ihre Sozialversicherungsnummer und Ihr Geburtsdatum anzugeben.

Was tun Sie?

Nr. 4

Wählen Sie unten die beste Antwort aus.

A Sie nennen die gewünschten Informationen, weil Sie Ihr Kennwort zurücksetzen und mit Ihrer Arbeit fortfahren möchten.

B Sie fragen die Person nach ihrer E-Mail-Adresse und Telefonnummer, um ihre Identität zu überprüfen, und stellen dann die gewünschten Informationen bereit.

C Sie legen sofort auf und melden den Anruf Ihrer IT-Abteilung.

D Sie nennen Ihre Mitarbeiternummer und Ihr Geburtsdatum, aber nicht Ihre Sozialversicherungsnummer.

E Keine der oben genannten Antworten.

DELL Technologies

ANTWORT

Social Engineering

Nr. 4

GUT GEMACHT!

Auflegen und die IT kontaktieren!

Manche Angreifer versuchen, Sie durch Social Engineering am Telefon zu manipulieren und so an vertrauliche Informationen zu gelangen. Selbst wenn Sie in Ihrem System sehen können, dass die genannte Person ein/e MitarbeiterIn in Ihrem Unternehmen ist, wissen Sie nicht, ob diese Person auch am anderen Ende der Leitung sitzt. **Sie sollten Kennwortzurücksetzungen immer selbst vornehmen.**

Nächste Frage

DELL Technologies

ANTWORT

Social Engineering

Nr. 4

GEHACKT!!!

Auflegen und die IT kontaktieren!

Manche Angreifer versuchen, Sie durch Social Engineering am Telefon zu manipulieren und so an vertrauliche Informationen zu gelangen. Selbst wenn Sie in Ihrem System sehen können, dass die genannte Person ein/e MitarbeiterIn in Ihrem Unternehmen ist, wissen Sie nicht, ob diese Person auch am anderen Ende der Leitung sitzt. **Sie sollten Kennwortzurücksetzungen immer selbst vornehmen.**

Nächste Frage

DELL Technologies

FRAGE 5 VON 14

PC-Infiltrierung

Sie führen ein Telefonat und sehen, dass auf Ihrem Bildschirm etwas Seltsames vor sich geht. Die Maus bewegt sich von selbst, Text oder Konsolenfenster werden geöffnet und geschlossen oder Menüs werden unvermittelt ein- und ausgeblendet.

Was tun Sie?

Nr. 5

Wählen Sie unten die beste Antwort aus.

A Sie nehmen an, dass es sich um ein harmloses PC-Problem handelt, und setzen Ihre Arbeit fort.

B Sie sprechen die Angelegenheit bei Ihrer IT-Abteilung an, arbeiten aber trotzdem weiter.

C Sie stellen die Nutzung des PCs sofort ein, fahren ihn herunter und kontaktieren Ihre IT-Abteilung (mit einem anderen Gerät), um das Problem zu melden.

DELL Technologies

ANTWORT

PC-Infiltrierung

Nr. 5

GUT GEMACHT!

Sofort die IT kontaktieren!

Wenn sich Ihre Maus „von selbst“ auf dem Bildschirm bewegt, kann dies ein Anzeichen für einen ernsten Angriff mit Datenschutzverletzung und möglichem Keylogging sein. Ihre IT-Abteilung muss schnellstmöglich darüber informiert werden, um effektive Maßnahmen ergreifen zu können.

Nächste Frage

DELL Technologies

ANTWORT

PC-Infiltrierung

Nr. 5

GEHACKT!!!

Sofort die IT kontaktieren!

Ungewöhnliches Verhalten kann darauf hindeuten, dass ein Angreifer Ihren PC überwacht und womöglich Daten exfiltriert und Tastatureingaben erfasst, darunter auch Ihre Kennwörter und andere wichtige Informationen. Am besten fahren Sie den PC herunter und melden das Problem Ihrer IT-Abteilung.

Nächste Frage

DELL Technologies

FRAGE 6 VON 14

USB-gestützter Malware-Angriff

Sie laufen über den Parkplatz Ihres Unternehmens und bemerken eine Einkaufstüte zwischen zwei Fahrzeugen. Sie schauen hinein und sehen 5 USB-Sticks mit jeweils 500 GB. Sie sind versiegelt und noch originalverpackt.

Was tun Sie?

Nr. 6

Wählen Sie unten die beste Antwort aus.

A Sie öffnen eine Verpackung und stecken den USB-Stick in Ihren PC. Die anderen vier verteilen Sie an Ihre KollegInnen.

B Sie nehmen sie mit nach Hause und verwenden die USB-Sticks mit Ihrem privaten Computer.

C Sie benachrichtigen das Sicherheitspersonal und die IT-Abteilung über den Fund und übergeben ihnen die USB-Sticks.

D Sie verschenken die USB-Sticks zu Weihnachten an Ihre Kinder.

E Keine der oben genannten Antworten.

DELL Technologies

ANTWORT

USB-gestützter Malware-Angriff

Nr. 6

GUT GEMACHT!

Sicherheitspersonal und IT benachrichtigen!

Diese Art von Angriff ermöglicht Angreifern das Platzieren von Malware in einem Unternehmen, wobei ein/e MitarbeiterIn unbeabsichtigt als „BotIn“ fungiert und die bösartige Payload in das Netzwerk bringt. Stecken Sie niemals einen USB-Stick oder sonstiges Zubehör unbekannter Herkunft in IRGENDEINES Ihrer Geräte. Und als Geschenk eignen sie sich dementsprechend natürlich auch nicht.

Nächste Frage

DELL Technologies

ANTWORT

USB-gestützter Malware-Angriff

Nr. 6

GEHACKT!!!

Sicherheitspersonal und IT benachrichtigen!

Diese Art von Angriff ermöglicht Angreifern das Platzieren von Malware in einem Unternehmen, wobei ein/e MitarbeiterIn unbeabsichtigt als „BotIn“ fungiert und die bösartige Payload in das Netzwerk bringt. Stecken Sie niemals einen USB-Stick oder sonstiges Zubehör unbekannter Herkunft in IRGENDEINES Ihrer Geräte. Und als Geschenk eignen sie sich dementsprechend natürlich auch nicht.

Nächste Frage

DELL Technologies

FRAGE 7 VON 14

Ransomware

Ein/e VerkäuferIn kommt in Ihr Büro und präsentiert neue Technologie, an der Ihr Unternehmen interessiert ist. Die Präsentation befindet sich auf einem USB-Stick, den Sie auf Bitte des/der VerkäuferIn in Ihren PC stecken sollen, damit die Präsentation mit einem Projektor gezeigt werden kann, während die Person spricht.

Was tun Sie?

Nr. 7

Wählen Sie unten die beste Antwort aus.

A Sie tun, worum Sie gebeten wurden, und stecken den USB-Stick in Ihren PC.

B Sie fragen, ob die Präsentation heruntergeladen werden kann, da Ihre Unternehmensrichtlinie die Verwendung externer USB-Sticks untersagt. Wenn das Herunterladen aber nicht möglich ist, tun Sie, worum Sie gebeten wurden, und stecken den USB-Stick in Ihren PC.

C Sie bitten die Person, die Präsentation ohne Projektor abzuhalten, und stecken den USB-Stick nicht in Ihren PC.

D Sie vergewissern sich, dass die Person den USB-Strick nicht auf einem Parkplatz gefunden hat, und stecken ihn dann in Ihren PC.

E Sie fertigen zusätzliche Kopien des USB-Sticks an und übergeben eine davon an Ihre/n ManagerIn.

DELL Technologies

ANTWORT

Ransomware

Nr. 7

GUT GEMACHT!

Den USB-Stick nicht einstecken und auf die Präsentation verzichten!

Sie wissen nichts davon, aber dem/der VerkäuferIn wurde eine beträchtliche Summe als Bestechungsgeld angeboten und der USB-Stick enthält eine Ransomware-Payload, die Ihre Systeme sperren wird. Doch da Sie den USB-Stick nicht eingesteckt und auch keine anderen Dateien heruntergeladen haben, haben Sie verhindert, dass der/die AngreiferIn Zugang erhält. Glück gehabt!

Nächste Frage

DELL Technologies

ANTWORT

Ransomware

Nr. 7

GEHACKT!!!

Den USB-Stick nicht einstecken und auf die Präsentation verzichten!

Sie wissen nichts davon, aber dem/der VerkäuferIn wurde eine beträchtliche Summe als Bestechungsgeld angeboten und der USB-Stick enthält eine Ransomware-Payload, die Ihre Systeme sperren wird. Verwenden Sie keine externen USB-Sticks und laden Sie keine Dateien aus unbekannten Quellen auf Ihren privaten oder unternehmenseigenen PC herunter.

Nächste Frage

DELL Technologies

FRAGE 8 VON 14

Zwei-Faktor-Authentifizierung

Ihre Bank hat empfohlen, für die Anmeldung auf ihrer Website die Zwei-Faktor-Authentifizierung zu verwenden. Auch andere Websites verwenden diesen Prozess zum Gewährleisten der Nutzersicherheit.

Welche der folgenden Optionen ist ein Beispiel für die Zwei-Faktor-Authentifizierung?

Nr. 8

Wählen Sie unten die beste Antwort aus.

A Sie geben Ihren Nutzernamen und Ihr Kennwort ein und werden dann aufgefordert, Ihre PIN anzugeben, um Zugriff auf die Website zu erhalten.

B Sie geben Ihren Nutzernamen und Ihr Kennwort ein und lösen einen CAPTCHA, bei dem Sie die Kacheln wählen müssen, die Schilder enthalten.

C Sie geben Ihren Nutzernamen und Ihr Kennwort ein und die Website sendet eine Textnachricht mit einem Einmalcode an Ihr Mobiltelefon, den Sie im entsprechenden Feld auf der Website eingeben müssen.

D Sie geben Ihren Nutzernamen ein und die Website verlangt von Ihnen die Eingabe eines Codes unter Verwendung eines sicheren Tokens, das sich jede Minute ändert und auf Ihrem Telefon installiert ist.

E Nur A und C.

F Nur C und D.

G Keine der oben genannten Antworten.

DELL Technologies

ANTWORT

Zwei-Faktor-Authentifizierung

Nr. 8

GUT GEMACHT!

Sie brauchen beides!

Die Zwei-Faktor-Authentifizierung erfordert sowohl ein Kennwort als auch eine andere, zweite Kennung für die Identifizierung und Authentifizierung von NutzerInnen, z. B. einen per Textnachricht versendeten Code oder eine von einer App generierte Zahl. Durch diese Sicherheitsebene wird es für Angreifer weitaus schwieriger, Zugriff auf Ihre Daten zu erhalten.

Nächste Frage

DELL Technologies

ANTWORT

Zwei-Faktor-Authentifizierung

Nr. 8

GUT GEMACHT, ABER ...

Sie brauchen beides!

Sie sind nah dran! Unter den Antworten gibt es zwei Beispiele für die Zwei-Faktor-Authentifizierung. Versuchen Sie noch einmal, die zweite Option zu finden.

Nächste Frage

DELL Technologies

ANTWORT

Zwei-Faktor-Authentifizierung

Nr. 8

GEHACKT!!!

Hoppla! Sie brauchen beides!

Die Zwei-Faktor-Authentifizierung erfordert sowohl ein Kennwort als auch eine andere, zweite Kennung für die Identifizierung und Authentifizierung von NutzerInnen, z. B. einen per Textnachricht versendeten Code oder eine von einer App generierte Zahl. Durch diese Sicherheitsebene wird es für Angreifer weitaus schwieriger, Zugriff auf Ihre Daten zu erhalten. Ohne die Zwei-Faktor-Authentifizierung sind Sie anfällig für Angriffe.

Nächste Frage

DELL Technologies

FRAGE 9 VON 14

Bluetooth-Diebstahl

Sie sind zu einem Wanderparkplatz gefahren und wollen sich zu Fuß auf den Weg machen. Da bemerken Sie, dass Ihr Laptop noch in Ihrem Rucksack ist, und Sie haben auch Ihr Telefon dabei, das aber keinen Empfang hat. Sie müssen Ihren Computer und Ihr Telefon im Wagen lassen, wollen aber keine Sicherheitsrisiken eingehen.

Was tun Sie?

Nr. 9

Wählen Sie unten die beste Antwort aus.

A Sie schalten überall das Wi-Fi aus.

B Sie versetzen Ihren Laptop in den Ruhemodus.

C Sie sperren Ihren Laptop und Ihr Telefon in den Kofferraum.

D Sie wickeln Ihren Laptop und Ihr Telefon in eine dicke Decke.

E Sie schalten Ihren Laptop und Ihr Telefon komplett aus, sodass auch die Bluetooth-Funktion ausgeschaltet wird.

DELL Technologies

ANTWORT

Bluetooth-Diebstahl

Nr. 9

GUT GEMACHT!

Laptop und Telefon ausschalten!

Natürlich ist es immer am besten, Ihre Geräte nicht sichtbar liegen zu lassen, wenn Sie nicht da sind. Doch Diebe verwenden Bluetooth-Scanner, um Geräte in abgeschlossenen Fahrzeugen ausfindig zu machen – und es ist nicht bei allen Geräten so, dass im Ruhemodus auch die Bluetooth-Funktion deaktiviert wird. Diebstähle passieren oft auf Wanderparkplätzen und an anderen Orten, wo die BesitzerInnen für einen längeren Zeitraum weg sind – und Diebe halten immer die Augen offen. Seien Sie also achtsam, bevor Sie zum Wandern aufbrechen.

Nächste Frage

DELL Technologies

ANTWORT

Bluetooth-Diebstahl

Nr. 9

GEHACKT!!!

Laptop und Telefon ausschalten!

Natürlich ist es immer am besten, Ihre Geräte nicht sichtbar liegen zu lassen, wenn Sie nicht da sind. Doch Diebe verwenden Bluetooth-Scanner, um Geräte in abgeschlossenen Fahrzeugen ausfindig zu machen – und es ist nicht bei allen Geräten so, dass im Ruhemodus auch die Bluetooth-Funktion deaktiviert wird. Diebstähle passieren oft auf Wanderparkplätzen und an anderen Orten, wo die BesitzerInnen für einen längeren Zeitraum weg sind. Seien Sie also achtsam, bevor Sie zum Wandern aufbrechen.

Nächste Frage

DELL Technologies

FRAGE 10 VON 14

USB-Angriff, Teil 2

Sie sind in festlicher Stimmung und bringen einen über USB betriebenen Mini-Weihnachtsbaum mit ins Büro.

Wie gehen Sie für die Stromversorgung vor?

Nr. 10

Wählen Sie unten die beste Antwort aus.

A Sie schließen ihn an Ihren PC an.

B Sie schließen ihn an einen USB-Extender an, der mit Ihrem PC verbunden ist.

C Sie verwenden ein dediziertes USB-Ladegerät, um den Baum an eine gewöhnliche Steckdose anzuschließen.

D Sie können den Weihnachtsbaum nicht mit Strom versorgen, Weihnachten fällt aus.

E Keine der oben genannten Antworten.

DELL Technologies

ANTWORT

USB-Angriff, Teil 2

Nr. 10

GUT GEMACHT!

Ein dediziertes USB-Ladegerät verwenden!

Bei einem USB-basierten Angriff dieser Art wird Malware auf verschiedenste Geräte geladen – sogar auf kleine Weihnachtsbäume. Dies geschieht in der Hoffnung, dass sie mit einem wertvollen Unternehmensnetzwerk verbunden werden. Schließen Sie niemals ein unbekanntes USB-Gerät an Ihren PC an – auch nicht, wenn Sie es einfach nur aufladen möchten.

Nächste Frage

DELL Technologies

ANTWORT

USB-Angriff, Teil 2

Nr. 10

GEHACKT!!!

Ein dediziertes USB-Ladegerät verwenden!

Bei einem USB-basierten Angriff dieser Art wird Malware auf verschiedenste Geräte geladen – sogar auf kleine Weihnachtsbäume. Dies geschieht in der Hoffnung, dass sie mit einem wertvollen Unternehmensnetzwerk verbunden werden. Schließen Sie niemals ein unbekanntes USB-Gerät an Ihren PC an – auch nicht, wenn Sie es einfach nur aufladen möchten.

Nächste Frage

DELL Technologies

FRAGE 11 VON 14

Evil-Maid-Angriff

Sie sind wegen einer Cybersicherheitskonferenz in Shanghai, China, und übernachten in einem 5-Sterne-Hotel. Bevor Sie sich auf den Weg zum Abendessen machen, schließen Sie Ihren PC in den Safe in Ihrem Zimmer.

Ist Ihr PC vor Angriffen und Diebstahl geschützt?

Nr. 11

Wählen Sie unten die beste Antwort aus.

A Nein, da jedes unbeaufsichtigte Gerät kompromittiert werden kann.

B Ja, da Sie ihn sicher im Safe eingeschlossen haben.

C Ja, schließlich haben Sie auch Kleidung im Schrank aufgehängt, um den Safe zu verstecken.

D Ja, schließlich sind Sie in einem sehr gehobenen Hotel.

E Ja, denn es handelt sich nicht um einen besonders ansprechenden PC.

DELL Technologies

ANTWORT

Evil-Maid-Angriff

Nr. 11

GUT GEMACHT!

Nein, jedes Gerät kann kompromittiert werden!

Jedes unbeaufsichtigt gelassene Gerät kann geöffnet und kompromittiert werden. Man spricht hier vom „Evil-Maid-Angriff“, bei dem Angreifer sich Zugriff verschaffen, indem sie den PC physisch öffnen, um Malware einzuschleusen. Ein Gerät, das Sie nicht bei sich haben, ist immer anfällig für Angriffe. Sie sollten Ihr Gerät auch niemals in der Obhut unbekannter Personen lassen – vor allem, wenn es sich um übel gesinnte Mitmenschen handelt.

Nächste Frage

DELL Technologies

ANTWORT

Evil-Maid-Angriff

Nr. 11

GEHACKT!!!

Nein, jedes Gerät kann kompromittiert werden!

Jedes unbeaufsichtigt gelassene Gerät kann geöffnet und kompromittiert werden. Man spricht hier vom „Evil-Maid-Angriff“, bei dem Angreifer sich Zugriff verschaffen, indem sie den PC physisch öffnen, um Malware einzuschleusen. Um Sicherheit gewährleisten zu können, müssen Sie ihre Geräte bei sich haben. Lassen Sie Ihr Gerät niemals in der Obhut unbekannter Personen – vor allem, wenn es sich um übel gesinnte Mitmenschen handelt.

Nächste Frage

DELL Technologies

Spyware

Sie erhalten eine Textnachricht von einer Nummer, die ihnen irgendwie bekannt vorkommt, und werden darüber informiert, dass Ihre Tochter einen Unfall hatte und ins Krankenhaus gebracht wurde. Die Nachricht enthält einen Link zur direkten Kontaktaufnahme.

Was tun Sie?

Nr. 12

Wählen Sie unten die beste Antwort aus.

A Sie klicken sofort auf den Link, da Sie sich Sorgen um Ihre Tochter machen.

B Sie schlagen die Nummer nach, sehen, dass sie zu dem Gebiet gehört, wo Ihre Tochter unterwegs war, und klicken dann auf den Link.

C Sie klicken nicht auf den Link, sondern schicken Ihrer Tochter eine Nachricht, um sicherzugehen, dass es ihr gut geht.

D Keine der oben genannten Antworten.

DELL Technologies

ANTWORT

Spyware

Nr. 12

GUT GEMACHT!

Nicht auf den Link klicken!

Diese Art von Angriff ist ein Versuch, Spyware auf Ihrem Telefon zu platzieren. Diese kann Ihr Telefon kompromittieren und sich möglicherweise anschließend im Unternehmensnetzwerk ausbreiten. Sie haben erkannt, dass etwas nicht stimmt, und haben auf andere Weise sichergestellt, dass bei Ihrer Tochter alles in Ordnung ist. Gut gemacht!

Nächste Frage

DELL Technologies

ANTWORT

Spyware

Nr. 12

GEHACKT!!!

Nicht auf den Link klicken!

Diese Art von Angriff ist ein Versuch, Spyware auf Ihrem Telefon zu platzieren. Diese kann Ihr Telefon kompromittieren und sich möglicherweise anschließend im Unternehmensnetzwerk ausbreiten. Durch Klicken auf den Link landet eine Spyware-Payload auf Ihrem Gerät. Fallen Sie nicht auf trügerische Textnachrichten herein, ganz gleich, wie überzeugend sie sind.

Nächste Frage

DELL Technologies

FRAGE 13 VON 14

Endpoint Security

Bedrohungsakteure (man kann sie auch als Hacker mit bösartigen Absichten bezeichnen) nehmen Endpunkte ins Visier.

Endpunkte sind per Definition:

Nr. 13

Wählen Sie unten die beste Antwort aus.

A	Desktop-PCs.
B	Desktop-PCs und Laptops.
C	Desktop-PCs, Laptops und Server.
D	Desktop-PCs, Laptops, Server, die Cloud und mehr.
E	Desktop-PCs, Laptops, Server, die Cloud und das letzte Ziel auf meinem Navigationsgerät.

DELL Technologies

ANTWORT

Endpoint Security

Nr. 13

GUT GEMACHT!

Jedes remote verbundene Gerät!

Ein Endpunkt ist ein beliebiges Gerät, das remote mit einem Netzwerk verbunden ist. Die Endpoint Security ist für den Schutz der Geräte und Daten in Ihrem Unternehmen unerlässlich – sorgen Sie also dafür, dass Sie Angreifern einen Schritt voraus bleiben!

Nächste Frage

DELL Technologies

ANTWORT

Endpoint Security

Nr. 13

GUT GEMACHT, ABER ...

Jedes remote verbundene Gerät!

Ein Endpunkt ist ein beliebiges Gerät, das remote mit einem Netzwerk verbunden ist. Die Endpoint Security ist für den Schutz der Geräte und Daten in Ihrem Unternehmen unerlässlich – sorgen Sie also dafür, dass Sie Angreifern einen Schritt voraus bleiben!

Nächste Frage

DELL Technologies

ANTWORT

Endpoint Security

Nr. 13

GEHACKT!!!

Jedes remote verbundene Gerät!

Ein Endpunkt ist ein beliebiges Gerät, das remote mit einem Netzwerk verbunden ist. Die Endpoint Security ist für den Schutz der Geräte und Daten in Ihrem Unternehmen unerlässlich – sorgen Sie also dafür, dass Sie Angreifern einen Schritt voraus bleiben!

Nächste Frage

DELL Technologies

FRAGE 14 VON 14

Endpoint Security, Teil 2

Hacker mit bösartigen Absichten nehmen Endpunkte wie Desktop-PCs, Laptops, Mobiltelefone, kabellose Drucker und Server ins Visier – im Grunde alles, was sich mit einem Netzwerk verbindet.

Welche Schritte sollten Sie unternehmen, um einen Angriff zu vermeiden?

Nr. 14

Wählen Sie unten die beste Antwort aus.

A Sicherstellen, dass ich mein Gerät sperre und wegsperre, wenn ich es nicht verwende.

B Mein Gerät regelmäßig aktualisieren und patchen.

C Auf eine gute E-Mail-Hygiene achten und verdächtige E-Mails melden.

D Niemals ein unbekanntes Gerät an meinen Endpunkt anschließen.

E Alle oben genannten Antworten.

DELL Technologies

ANTWORT

Endpoint Security, Teil 2

Nr. 14

GUT GEMACHT!

Alle oben genannten Antworten!

Sie wissen, worauf es in Bezug auf Cybersicherheit ankommt, und können Ihr Wissen in die Tat umsetzen. Die Endpoint Security ist für den Schutz der Geräte und Daten in Ihrem Unternehmen unerlässlich – sorgen Sie also dafür, dass Sie Angreifern einen Schritt voraus bleiben!

Nächste Frage

DELL Technologies

ANTWORT

Endpoint Security, Teil 2

Nr. 14

GUT GEMACHT, ABER ...

Sie können noch mehr tun!

Zum Schutz Ihrer Geräte müssen Sie mehr als nur eine Sache tun. Die Endpoint Security ist für den Schutz der Geräte und Daten in Ihrem Unternehmen unerlässlich – sorgen Sie also dafür, dass Sie Angreifern einen Schritt voraus bleiben!

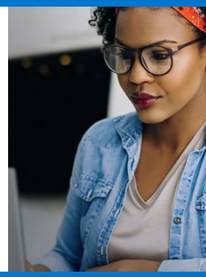
Nächste Frage

DELL Technologies

VIELEN DANK!

Weitere Informationen:

Besuchen Sie **Dell.com/Endpoint-Security**



DELL Technologies