DELL Technologies

サイバー攻撃への対策はできていますか？

テストの開始

問題1（全14問）

フィッシング

あなたは「Windows Defenderの注文」というEメールを受信しました。正規のドキュメントのように見える請求書が添付され、Microsoft Defenderアカウントの1年間のサブスクリプションの料金399.99ドルが請求されています。「このメールには返信しないでください」と明記されていますが、［ヘルプとお問い合わせ］ボタンがあり、電話番号も記載されています。あなたはこのような注文をした覚えがありません。

どのように対応しますか？

#1

最も適切な回答を選択してください

A この料金をクレジット カードに請求されたくないので、すぐに［ヘルプとお問い合わせ］ボタンをクリックする。

B Webブラウザーのシークレット モードでEメールを開いてから［ヘルプとお問い合わせ］ボタンをクリックする。

C クレジット カードのオンライン明細を見て、請求されているかどうかを確認する。その後、詳細を確認するため、記載の電話番号に問い合わせてみる。

D Eメール アドレスをよく見るとフィッシング メールのようだったので、Eメール プログラムの［フィッシングを報告］をクリックし、調査のためIT部門にもメールを転送する。もちろんメールは開かない。

E Eメールを開かずに削除する。

DELL Technologies

回答

フィッシング

#1

正解です！

フィッシングを報告してください！

疑わしいEメールが届き、何かの理由でリンクをクリックするよう求められる場合、最善の行動は、Eメールを開かずに削除するか、Outlookメニュー バーの［フィッシングを報告］をクリックして、調査のためIT部門に報告することです。**フィッシングと思われるメールは、おそらくフィッシングで間違いありません。**

次の質問

DELL Technologies

回答

フィッシング

#1

よくできましたが、
不正解です。

フィッシングを報告してください！

怪しいと思われる電話番号に電話することには、やはりリスクがあります。他の選択肢の中に、もっとよい解決方法があります。

フィッシングと思われるメールは、おそらくフィッシングで間違いありません。

次の質問

DELL Technologies

回答

フィッシング

#1

ハッキングされました！

フィッシングを報告してください！

疑わしいEメールが届き、何かの理由でリンクをクリックするよう求められる場合、最善の行動は、Eメールを開かずに削除するか、Outlookメニュー バーの［フィッシングを報告］をクリックして、調査のためIT部門に報告することを忘れないでください。**フィッシングと思われるメールは、おそらくフィッシングで間違いありません。**

次の質問

DELL Technologies

問題2（全14問）

ソーシャル メディア フィッシング

Instagramアカウントを見てみると、有名な歌手の投稿に書き込んだあなたのコメントに対して、歌手本人からの返信が直接届いていました！ダイレクトメッセージで連絡してくださいと書かれており、貴重な限定コンテンツへのリンクが含まれていました。

どのように対応しますか？

#2

最も適切な回答を選択してください

A 信じられないほどの幸運に恵まれたので、すぐにリンクをクリックする。

B リンクをコピーして、シークレット モードで開く。

C ソーシャル メディアで友達にリンクをシェアする。

D リンクにマウス カーソルを合わせるとフィッシングのように思えたので、メッセージを削除し、送信者をブロックする。

E 何もクリックせず、送信者をブロックし、報告する。

DELL Technologies

回答

ソーシャル メディア フィッシング

#2

正解です！

フィッシングを報告してください！

疑わしいEメールが届き、何かの理由でリンクをクリックするよう求められる場合、最善の行動は、Eメールを開かずに削除するか、Outlookメニュー バーの［フィッシングを報告］をクリックして、調査のためIT部門に報告することです。**フィッシングと思われるメールは、おそらくフィッシングで間違いありません。**

次の質問

DELL Technologies

回答

ソーシャル メディア フィッシング

#2

ハッキングされました！

フィッシングを報告してください！

疑わしいEメールが届き、何かの理由でリンクをクリックするよう求められる場合、最善の行動は、Eメールを開かずに削除するか、Outlookメニュー バーの［フィッシングを報告］をクリックして、調査のためIT部門に報告することを忘れないでください。**フィッシングと思われるメールは、おそらくフィッシングで間違いありません。**

次の質問

DELL Technologies

問題3（全14問）

パスワード セキュリティ

社内のIT部門が、強いパスワードを設定するように要求しています。パスワードのような「認証情報」は、攻撃者が探し求める、最も価値のあるターゲットの1つだからです。では…

パスワードの安全性を高めるにはどうすればよいでしょうか？

#3

最も適切な回答を選択してください

A 少なくとも8文字、できればそれ以上の文字数のパスワードにする。

B 英字、数字、記号を組み合わせて使う。

C 異なるアカウントやサイトで同じパスワードを使い回さない（それぞれパスワードを別にする）。

D 上記すべて。

E 上記以外。

DELL Technologies

回答

パスワード セキュリティ

#3

正解です！

強いパスワードを使いましょう！

安全なパスワードは、英字、数字、記号を組み合わせた8文字以上の一意のパスワードです。固有の覚えやすいパスフレーズを使用してもよいでしょう。ただし、ペットの名前は使用しないでください。また、2要素認証を必ず使用してください。2要素認証と強いパスワードを併用することで、最適な保護が得られます。

次の質問

DELL Technologies

回答

パスワード セキュリティ

#3

よくできましたが、
不正解です。

強いパスワードを使いましょう！

安全なパスワードは、上記のセキュリティ対策をすべて組み合わせたものです。英字、数字、記号を組み合わせた8文字以上の一意のパスワードにします。ただし、ペットの名前は使用しないでください。セキュリティをさらに高めるには、2要素認証や、パスワードの代わりとして数字と文字を組み合わせたパスフレーズを使用します。

次の質問

DELL Technologies

回答

パスワード セキュリティ

#3

ハッキングされました！

強いパスワードを使いましょう！

安全なパスワードは、英字、数字、記号を組み合わせた8文字以上の一意のパスワードです。セキュリティをさらに高めるには、2要素認証や、パスワードの代わりとして数字と文字を組み合わせたパスフレーズを使用します。

次の質問

DELL Technologies

問題4（全14問）

ソーシャル エンジニアリング

あなたの携帯電話にIT部門を名乗る人から電話がかかってきました。パスワードの期限が切れるため、新しいパスワードを設定する必要があると言われました。電話の相手は、認証するために社員番号、社会保障番号、生年月日を教えてほしいと言っています。

どのように対応しますか？

#4

最も適切な回答を選択してください

A パスワードをリセットしてまた使えるようにしたいので、要求された情報を伝える。

B 相手の身元を確認するため、連絡先のEメール アドレスと電話番号を聞き出し、その後で要求された情報を伝える。

C すぐに通話を切り、IT部門に報告する。

D 社員番号と生年月日は教える。ただし、社会保障番号については教えない。

E 上記以外。

DELL Technologies

回答

ソーシャル エンジニアリング

#4

正解です！

電話を切って、IT部門に報告してください！

ソーシャル エンジニアリングを使用して、電話であなたから個人情報を聞き出すように誘導する攻撃者がいます。社内に同じ名前の従業員がいると確認できた場合でも、電話で話している相手が本人であるという保証はありません。**パスワードのリセットは必ず自分で行ってください。**

次の質問

DELL Technologies

回答

ソーシャル エンジニアリング

#4

ハッキングされました！

電話を切って、IT部門に報告してください！

ソーシャル エンジニアリングを使用して、電話であなたから個人情報を聞き出すように誘導する攻撃者がいます。社内に同じ名前の従業員がいると確認できた場合でも、電話で話している相手が本人であるという保証はありません。パスワードのリセットは必ず自分で行ってください。

次の質問

DELL Technologies

問題5（全14問）

パソコンへの侵入

通話中に、パソコンの画面の挙動がおかしいことに気がつきました。マウス カーソルが勝手に動き、テキストやコンソールのウィンドウが開いたり閉じたり、メニューが表示されたり消えたりしています。

どのように対応しますか？

#5

最も適切な回答を選択してください

A パソコンの不具合で特に害はないと判断して仕事を続ける。

B この件をIT部門に確認して、仕事は続ける。

C すぐにパソコンの使用を中止し、シャットダウンする。さらに、（別のデバイスを使って）IT部門に連絡し、問題を報告する。

DELL Technologies

回答

パソコンへの侵入

#5

正解です！

IT部門にただちに連絡してください！

画面のマウス カーソルが「勝手に」動いているということは、データ侵害やキー ロギングなど重大な攻撃が行われている可能性があることを示しています。IT部門は、この件をできるだけ早急に把握して、有効な対策を実施する必要があります。

次の質問

DELL Technologies

回答

パソコンへの侵入

#5

ハッキングされました！

IT部門にただちに連絡してください！

異常な挙動が見られる場合、攻撃者にパソコンが監視されている可能性があります。データが抜き出され、パスワードやその他の重要な情報を含むキー入力も記録されているかもしれません。最適な対応策は、ただちにパソコンをシャットダウンして、問題をIT部門に報告することです。

次の質問

DELL Technologies

問題6（全14問）

USBを使用したマルウェア攻撃

会社の駐車場を歩いていると、車の間にショッピング バッグが置いてありました。中にはUSBドライブが5個入っていました。パッケージは未開封で、それぞれ500GBの容量です！

どのように対応しますか？

#6

最も適切な回答を選択してください

A 1つを開封して、自分のパソコンのUSBスロットに挿入する。残りの4つは同僚にあげる。

B 全部家に持ち帰り、自宅のパソコンでUSBドライブを使用する。

C USBドライブを見つけたことを建物の警備員とIT部門に知らせ、後の処置を任せる。

D このUSBドライブは子どもたちへのプレゼントにする。

E 上記以外。

DELL Technologies

回答

USBを使用したマルウェア攻撃

#6

正解です！

警備員とIT部門に知らせてください！

このような攻撃では、攻撃者が組織にマルウェアを仕掛けることができます。従業員は「運び屋」として使われ、悪意あるプログラムがネットワークに入り込んでしまうのです。出どころのわからないUSBドライブなどの周辺機器は、所持するデバイスに一切挿入してはいけません。人にあげたら最悪のプレゼントになってしまいます！

次の質問

DELL Technologies

回答

USBを使用したマルウェア攻撃

#6

ハッキングされました！

警備員とIT部門に知らせてください！

このような攻撃では、攻撃者が組織にマルウェアを仕掛けることができます。従業員は「運び屋」として使われ、悪意あるプログラムがネットワークに入り込んでしまうのです。出どころのわからないUSBドライブなどの周辺機器は、所持するデバイスに一切挿入してはいけません。人にあげたら最悪のプレゼントになってしまいます！

次の質問

DELL Technologies

問題7（全14問）

ランサムウェア

営業担当者がやってきて、あなたの会社で導入を検討している新技術についてプレゼンしようとしています。担当者はプレゼン資料が保存されているUSBドライブを持参してきました。その担当者から「プロジェクターで投影して説明するため、USBをパソコンに挿入していただけますでしょうか」と言われました。

どのように対応しますか？

#7

最も適切な回答を選択してください

A 言われたとおり、パソコンにUSBドライブを挿入する。

B 会社の規則で外部のUSBドライブの使用が禁止されているため、代わりにプレゼン資料をダウンロードできないかと確認する。ダウンロードできない場合は、言われたとおりにUSBドライブをパソコンに挿入する。

C プロジェクターを使わずにプレゼンを進めるように依頼し、USBはパソコンに挿入しない。

D そのUSBドライブは駐車場で拾ったものではないことを確認してからパソコンに挿入する。

E USBドライブのコピーをいくつか作成して、その1つを上司に渡す。

DELL Technologies

回答

ランサムウェア

#7

正解です！

プロジェクターは使わず、USBも挿入しないでください。

実は、この営業担当者は攻撃者に大金で雇われており、USBドライブの中にはシステムをロック ダウンさせるランサムウェアが入っていました。ただし、USBドライブを挿入せず、他のファイルもダウンロードしなければ、攻撃者のアクセスを防止できます。危ないところでした。

次の質問

DELL Technologies

回答

ランサムウェア

#7

ハッキングされました！

プロジェクターは使わず、USBも挿入しないでください。

実は、この営業担当者は攻撃者に大金で雇われており、USBドライブとファイルの両方にシステムをロック ダウンさせるランサムウェアが入っていました。外部のUSBドライブや、出どころのわからないダウンロード ファイルを、個人や会社のパソコンに入れてはいけません。

次の質問

DELL Technologies

問題8（全14問）

2要素認証

あなたが利用している銀行では、サイトにログインする際に2要素認証を利用するよう勧めています。他のWebサイトでも、ユーザーのセキュリティを確保するためにこのプロセスが使用されています。

2要素認証の例に当てはまるものは次のうちどれですか。

#8

最も適切な回答を選択してください

A Webサイトにアクセスする際に、ユーザー名とパスワードを入力し、それから暗証番号を入力するよう求められる。

B ユーザー名とパスワードを入力し、さらにCAPTCHAで該当する内容が含まれているパネルを選択する。

C ユーザー名とパスワードを入力すると、Webサイトから携帯電話にワンタイムコードが記載されたテキスト メッセージが送信される。Webサイト上のボックスにそのコードを入力する。

D ユーザー名を入力すると、1分ごとに更新されるセキュア トークンのコードを入力するようにWebサイトから求められる。セキュア トークンは、携帯電話にインストールされている。

E AとCのみ。

F CとDのみ。

G 上記以外。

DELL Technologies

回答

2要素認証

#8

正解です！

両方が必要です。

2要素認証は、パスワードの他に、テキスト メッセージで送信されるコードや、アプリが生成する番号などの識別子を要求して、ユーザーの識別と認証を行います。このセキュリティの層により、攻撃者が個人情報にアクセスするのがかなり難しくなります。

次の質問

DELL Technologies

回答

2要素認証

#8

よくできましたが、
不正解です。

両方が必要です。

もう少しでした。2要素認証の例は2つあります。再挑戦して、
もう1つの回答を探してみてください。

次の質問

DELL Technologies

回答

2要素認証

#8

ハッキングされました！

残念ですが、不正解です。
両方が必要です。

2要素認証は、パスワードの他に、テキスト メッセージで送信されるコードや、アプリが生成する番号などの識別子を要求して、ユーザーの識別と認証を行います。このセキュリティの層により、攻撃者が個人情報にアクセスするのがかなり難しくなります。使用しない場合、攻撃の対象になる可能性があります。

次の質問

DELL Technologies

問題9（全14問）

Bluetoothを使った窃盗

午後のハイキングに向かおうと車でハイキングコースの入口まで来たところ、バックパックにまだノートパソコンが入ったままで、携帯電話も持っていることに気づきました（ただし圏外）。あなたはコンピューターと携帯電話を車内に置いて行きたいのですが、安全も確保したいと考えています。

どのように対応しますか？

#9

最も適切な回答を選択してください

A Wi-Fiをすべてオフにする。

B ノートパソコンをスリープ モードにする。

C ノートパソコンと携帯電話をトランクに入れてロックする。

D ノートパソコンと携帯電話を厚手の毛布でくるんでおく。

E ノートパソコンと携帯電話の電源を完全に切り、Bluetoothをオフにする。

DELL Technologies

回答

Bluetoothを使った窃盗

#9

正解です！

ノートパソコンと携帯電話の電源を切りましょう！

デバイスから離れるときは、人目に触れないようにしておくことが最善の策です。ただし、犯罪者はBluetoothスキャナーを使用して、鍵のかかった車内にあるデバイスを探し出します。また、「スリープ モード」にしていても、Bluetoothがオフにならないデバイスもあります。窃盗は、ハイキングコースの入口など、持ち主が長時間離れるとわかっている場所でよく発生します。犯罪者には常に見られていると思ってください！ハイキングに出かける前は十分に注意しましょう！

次の質問

DELL Technologies

回答

Bluetoothを使った窃盗

#9

ハッキングされました！

ノートパソコンと携帯電話の電源を切りましょう！

デバイスから離れるときは、人目に触れないようにしておくことが最善の策です。ただし、犯罪者はBluetoothスキャナーを使用して、鍵のかかった車内にあるデバイスを探し出します。また、「スリープ モード」にしていても、Bluetoothがオフにならないデバイスもあります。窃盗は、登山口など、持ち主が長時間離れるとわかっている場所でよく発生します。ハイキングに出かける前は十分に注意しましょう！

次の質問

DELL Technologies

問題10（全14問）

USB攻撃パート2

クリスマス シーズンが近づいてきたので、USB給電式のミニ クリスマス ツリーをオフィスに飾りました。

電源はどうしますか？

#10

最も適切な回答を選択してください

A パソコンに接続する。

B USBの延長ケーブルを使用してパソコンに接続する。

C 専用のUSB充電器を使用して、通常の電源コンセントに接続する。

D 電源が使えないので、クリスマスはなしにする。

E 上記以外。

DELL Technologies

回答

USB攻撃パート2

#10

正解です！

専用のUSB充電器を使用しましょう！

USBを使ったこのような攻撃では、多数のデバイスにマルウェアが仕込まれています。小さなクリスマス ツリーも例外ではありません！企業の重要なネットワークに差し込まれるチャンスを狙っているのです。たとえ充電のためだけとしても、出どころのわからないUSBデバイスは絶対にパソコンに接続してはいけません。

次の質問

DELL Technologies

回答

USB攻撃パート2

#10

ハッキングされました！

専用のUSB充電器を使用しましょう！

USBを使ったこのような攻撃では、多数のデバイスにマルウェアが仕込まれています。小さなクリスマス ツリーも例外ではありません！企業の重要なネットワークに差し込まれるチャンスを狙っているのです。たとえ充電のためだけとしても、出どころのわからないUSBデバイスは絶対にパソコンに接続してはいけません。

次の質問

DELL Technologies

問題11（全14問）

悪意あるメイド

あなたは中国の上海で、サイバーセキュリティのカンファレンスに参加しており、5つ星のホテルに滞在中です。夕食に出かける前に、あなたはパソコンを部屋の金庫に入れて鍵をかけました。

このパソコンは、攻撃を受けたり盗難されたりするおそれがない状態でしょうか？

#11

最も適切な回答を選択してください

A　いいえ。手元にないデバイスはすべて侵害される可能性があります。

B　はい。金庫に入れて鍵をかけたので安全です。

C　はい。金庫が見えないように、クローゼットに衣服もかけておきました。

D　はい。かなり高級なホテルなので安全です。

E　はい。特に高いパソコンではないので心配ありません。

DELL Technologies

回答

悪意あるメイド

#11

正解です！

安全ではありません。手元にないデバイスは侵害される可能性があります！

手元にないデバイスは、開かれて侵害される可能性があります。これは一般に「悪意あるメイド」攻撃と呼ばれており、攻撃者が物理的に侵入してパソコンを開き、マルウェアを仕掛けるというものです。手元から離れたデバイスは、攻撃に対し無防備な状態です。また、見知らぬ人物にデバイスを預けてはいけません。特に「悪意あるメイド」には注意が必要です。

次の質問

DELL Technologies

回答

悪意あるメイド

#11

ハッキングされました！

安全ではありません。手元にないデバイスは侵害される可能性があります！

手元にないデバイスは、開かれて侵害される可能性があります。これは一般に「悪意あるメイド」攻撃と呼ばれており、攻撃者が物理的に侵入してパソコンを開き、マルウェアを仕掛けるというものです。安全を確保するためには、すべてのデバイスを持ち歩く必要があります。見知らぬ人物にデバイスを預けてはいけません。特に「悪意あるメイド」には注意が必要です。

次の質問

DELL Technologies

問題12（全14問）

スパイウェア

なんとなく見覚えのある番号からテキスト メッセージが届きました。メッセージには、あなたの娘が事故に巻き込まれ、病院に運ばれたと書かれています。すぐに連絡が取れるというリンクも記載されています。

どのように対応しますか？

#12

最も適切な回答を選択してください

A	娘の安否が心配なので、すぐにリンクをクリックする。
B	番号を調べたところ、娘のいる地域からかかってきていたので、リンクをクリックする。
C	リンクをクリックせずに、娘の無事を確認するため、娘本人にテキスト メッセージを送る。
D	上記以外。

DELL Technologies

回答

スパイウェア

#12

正解です！

リンクをクリックしてはいけません！

このタイプの攻撃では、あなたの携帯電話にスパイウェアを入れようとしています。このスパイウェアは、あなたの携帯電話を侵害し、社内ネットワークにまで拡散する可能性があります。何かおかしいことに気づき、他の方法を使って娘の無事を確認するのが正解です。正しい選択でした。

次の質問

DELL Technologies

回答

スパイウェア

#12

ハッキングされました！

リンクをクリックしてはいけません！

このタイプの攻撃では、あなたの携帯電話にスパイウェアを入れようとしています。このスパイウェアは、あなたの携帯電話を侵害し、社内ネットワークにまで拡散する可能性があります。リンクをクリックすると、あなたのデバイスにスパイウェアが入れられてしまいます。どれほど緊急を要する場合でも、送信元が不明なテキスト メッセージは無視しましょう。

次の質問

DELL Technologies

問題13（全14問）

エンドポイント セキュリティ

脅威アクター（悪意を持ったハッカー）はエンドポイントを狙っています。

エンドポイントの正しい定義を選択してください。

#13

最も適切な回答を選択してください

A デスクトップ。

B デスクトップとノートパソコン。

C デスクトップ、ノートパソコン、サーバー。

D デスクトップ、ノートパソコン、サーバー、クラウドなど。

E デスクトップ、ノートパソコン、サーバー、クラウド、GPSの前回の目的地。

DELL Technologies

回答

エンドポイント セキュリティ

#13

正解です！

リモート接続されているデバイスすべてが対象です！

エンドポイントとは、ネットワークにリモート接続されているすべてのデバイスを指します。組織のデバイスとデータを保護するために、エンドポイント セキュリティは必須です。攻撃者の先手を取りましょう！

次の質問

DELL Technologies

回答

エンドポイント セキュリティ

#13

よくできましたが、
不正解です。

リモート接続されているデバイスすべてが対象です！

エンドポイントとは、ネットワークにリモート接続されているすべてのデバイスを指します。組織のデバイスとデータを保護するために、エンドポイント セキュリティは必須です。攻撃者の先手を取りましょう！

次の質問

DELL Technologies

回答

エンドポイント セキュリティ

#13

ハッキングされました！

リモート接続されているデバイスすべてが対象です！

エンドポイントとは、ネットワークにリモート接続されているすべてのデバイスを指します。組織のデバイスとデータを保護するために、エンドポイント セキュリティは必須です。攻撃者の先手を取りましょう！

次の質問

DELL Technologies

問題14（全14問）

エンドポイント セキュリティ パート2

悪意のあるハッカーは、エンドポイントをターゲットとします。デスクトップ、ノートパソコン、携帯電話、ワイヤレス プリンター、サーバーなど、ネットワークに接続しているものすべてが攻撃の対象になります。

攻撃を防ぐためには、どのような手順を取ればよいでしょうか？

#14

最も適切な回答を選択してください

A 使用しないときは、必ずデバイスをロックし、鍵をかけて保管する。

B 定期的にデバイスをアップデートし、パッチを適用する。

C Eメールの管理をきちんと行い、疑わしいEメールは報告する。

D 出どころのわからないデバイスは、エンドポイントに接続しない。

E 上記すべて。

DELL Technologies

回答

エンドポイント セキュリティ パート2

#14

正解です！

すべてが当てはまります！

サイバーセキュリティの方法を学び、実践できるようになりました。組織のデバイスとデータを保護するために、エンドポイント セキュリティは必須です。攻撃者の先手を取りましょう！

次の質問

DELL Technologies

回答

エンドポイント セキュリティ パート2

#14

よくできましたが、
不正解です。

他にもするべきことがあります！

デバイスを保護するために必要なことは1つだけではありません。組織のデバイスとデータを保護するために、エンドポイントセキュリティは必須です。攻撃者の先手を取りましょう！

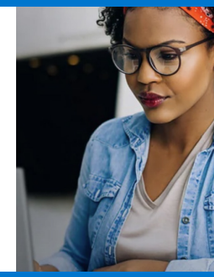
次の質問

DELL Technologies

ありがとうございました

詳細情報：

Dell.com/Endpoint-Securityにアクセス



DELL Technologies