DELL Technologies

Är du smartare än din cyberangripare?

Starta testet

FRÅGA 1 AV 14

Nätfiske

Du får ett e-postmeddelande från ”Windows Defender Order” med en faktura som ser officiell ut på 3 999 kr för en ettårsprenumeration på Microsoft Defender Account. Det står ”Svara inte på detta meddelande”, men det finns en Hjälp och kontakt-knapp och ett telefonnummer i meddelandet. Såvitt du minns har du inte beställt något sådant här.

Vad gör du?

Nr 1

Välj det bästa svaret nedan

A Du klickar omedelbart på Hjälp och kontakt-knappen, för du vill definitivt inte att ditt kreditkort ska debiteras för det här!

B Du öppnar meddelandet i ett inkognitofönster i webbläsaren och klickar på Hjälp och kontakt-knappen.

C Du kollar ditt kreditkortsutdrag online för att se om det har debiterats och ringer sedan telefonnumret för att försöka ta reda på mer.

D Du kontrollerar e-postadressen och upptäcker att den ser misstänkt ut, så du klickar på ”Rapportera nätfiske” genom e-postprogrammet och/eller vidarebefordrar meddelandet till din IT-avdelning så att de kan kolla upp det. Och du öppnar det så klart inte!

E Du raderar meddelandet utan att öppna det.

DELL Technologies

SVAR

Nätfiske

Nr 1

BRA JOBBAT!

Rapportera nätfiske!

När du får ett misstänkt e-postmeddelande där du blir ombedd att klicka på länkar, oavsett anledning, är det bäst att radera meddelandet utan att öppna det eller klicka på ”Rapportera nätfiske” i Outlook-fältet för att rapportera meddelandet till IT-avdelningen så att de kan kolla upp det. **Om det verkar misstänkt är det förmodligen det.**

Nästa fråga

DELL Technologies

SVAR

Nätfiske

Nr 1

BRA JOBBAT, MEN ...

Rapportera nätfiske!

Du utsätter fortfarande dig själv för risk genom att ringa vad som kommer att visa sig vara ett falskt nummer. Ett av de andra alternativen är bättre. **Om det verkar misstänkt är det förmodligen det.**

Nästa fråga

DELL Technologies

SVAR

Nätfiske

Nr 1

HACKAD!!!

Rapportera nätfiske!

Kom ihåg att när du får ett misstänkt e-postmeddelande där du blir ombedd att klicka på länkar, oavsett anledning, är det bäst att radera meddelandet utan att öppna det eller klicka på ”Rapportera nätfiske” i Outlook-fältet för att rapportera meddelandet till IT-avdelningen så att de kan kolla upp det. **Om det verkar misstänkt är det förmodligen det.**

Nästa fråga

DELL Technologies

FRÅGA 2 AV 14

Nätfiske på sociala medier

När du kollar ditt Instagram-konto ser du att Lyle Lovett har svarat på din kommentar på hans inlägg! Han skickar ett direktmeddelande till dig, med en länk som han ber dig klicka på för att komma åt väldigt begränsat och värdefullt innehåll.

Vad gör du?

Nr 2

Välj det bästa svaret nedan

A Du kan inte fatta vilken tur du har och klickar genast på länken.

B Du kopierar länken och öppnar den i ett inkognitofönster.

C Du delar länken med dina vänner på sociala medier.

D Du håller muspekaren över länken och misstänker att något skumt är på gång, så du raderar meddelandet och blockerar avsändaren.

E Du blockerar och rapporterar avsändaren utan att klicka på något.

DELL Technologies

SVAR

Nätfiske på sociala medier

Nr 2

BRA JOBBAT!

Rapportera nätfiske!

När du får ett misstänkt e-postmeddelande där du blir ombedd att klicka på länkar, oavsett anledning, är det bäst att radera meddelandet utan att öppna det eller klicka på ”Rapportera nätfiske” i Outlook-fältet för att rapportera meddelandet till IT-avdelningen så att de kan kolla upp det. **Om det verkar misstänkt är det förmodligen det.**

Nästa fråga

DELL Technologies

SVAR

Nätfiske på sociala medier

Nr 2

HACKAD!!!

Rapportera nätfiske!

Kom ihåg att när du får ett misstänkt e-postmeddelande där du blir ombedd att klicka på länkar, oavsett anledning, är det bäst att radera meddelandet utan att öppna det eller klicka på ”Rapportera nätfiske” i Outlook-fältet för att rapportera meddelandet till IT-avdelningen så att de kan kolla upp det.
Om det verkar misstänkt är det förmodligen det.

Nästa fråga

DELL Technologies

FRÅGA 3 AV 14

Säkra lösenord

Din IT-avdelning vill att du ska använda starka lösenord, och det är för att dessa inloggningsuppgifter är några av de värdefullaste saker som angripare är ute efter. Så ...

Hur kan du göra ditt lösenord säkrare?

Nr 3

Välj det bästa svaret nedan

A	Använda ett lösenord med minst åtta tecken, och helst fler.
B	Använda en kombination av bokstäver, siffror och specialtecken.
C	Undvika att använda samma lösenord för flera konton eller webbplatser. (Göra alla lösenord unika.)
D	Alla dessa.
E	Inga av dessa.

DELL Technologies

SVAR

Säkra lösenord

Nr 3

BRA JOBBAT!

Använd ett starkt lösenord!

Säkra lösenord är unika och kombinerar minst åtta bokstäver, siffror och specialtecken, och använder kanske till och med en unik lösenfras som du kommer ihåg. Och använd inte din hunds namn! Se även till att använda tvåfaktorsautentisering. Tillsammans med ett starkt lösenord ger det optimalt skydd.

Nästa fråga

DELL Technologies

SVAR

Säkra lösenord

Nr 3

BRA JOBBAT, MEN ...

Använd ett starkt lösenord!

Ett säkert lösenord kombinerar alla de angivna säkerhetsåtgärderna. Det är unikt och innehåller minst åtta bokstäver, siffror och specialtecken. Och använd inte din hunds namn! För extra säkerhet kan du använda tvåfaktorsautentisering och lösenfraser med siffror och specialtecken i stället för lösenord.

Nästa fråga

DELL Technologies

SVAR

Säkra lösenord

Nr 3

HACKAD!!!

Använd ett starkt lösenord!

Säkra lösenord är unika och kombinerar minst åtta bokstäver, siffror och specialtecken. För extra säkerhet kan du använda tvåfaktorsautentisering och lösenfraser med siffror och specialtecken i stället för lösenord.

Nästa fråga

DELL Technologies

FRÅGA 4 AV 14

Socialteknik

En person som säger att hen arbetar på din IT-avdelning ringer din mobil och säger att ditt lösenord har gått ut och att du behöver ange ett nytt lösenord. Telefonnumret ser säkert ut. Personen som ringer ber dig ange ditt personalnummer, personnummer och födelsedatum för verifieringssyften.

Vad gör du?

Nr 4

Välj det bästa svaret nedan

A Du anger informationen, för du vill återställa lösenordet så att du kan fortsätta jobba.

B Du ber om hens e-postadress och telefonnummer så att du kan verifiera vem hen är och ger sedan informationen i fråga.

C Du lägger genast på luren och rapporterar samtalet till din IT-avdelning.

D Du anger ditt personalnummer och födelsedatum, men håller ditt personnummer för dig själv.

E Inga av dessa.

DELL Technologies

SVAR

Socialteknik

Nr 4

BRA JOBBAT!

Lägg på luren och kontakta IT-avdelningen!

Vissa angripare använder socialteknik för att manipulera dig till att ge ut känslig information via telefon. Även om du kan verifiera att det är en medarbetare i systemet kan du inte vara säker på att det faktiskt är den personen du pratar med. **Du ska alltid inleda dina egna lösenordsåterställningar.**

Nästa fråga

DELL Technologies

SVAR

Socialteknik

Nr 4

HACKAD!!!

Lägg på luren och kontakta IT-avdelningen!

Vissa angripare använder socialteknik för att manipulera dig till att ge ut känslig information via telefon. Även om du kan verifiera att det är en medarbetare i systemet kan du inte vara säker på att det faktiskt är den personen du pratar med.

Du ska alltid inleda dina egna lösenordsåterställningar.

Nästa fråga

DELL Technologies

FRÅGA 5 AV 14

PC-infiltrering

När du svarar i telefon märker du att det pågår något skumt på din skärm. Musen rör på sig på egen hand, text eller konsolfönster öppnas och stängs eller menyer dyker upp och försvinner.

Så ...

Nr 5

Välj det bästa svaret nedan

A Du antar att det är ett harmlöst PC-problem och fortsätter arbeta.

B Du frågar IT-avdelningen om det, men fortsätter arbeta.

C Du slutar omedelbart använda din PC, stänger av den och kontaktar din IT-avdelning (på en annan enhet) för att rapportera problemet.

DELL Technologies

SVAR

PC-infiltrering

Nr 5

BRA JOBBAT!

Kontakta IT-avdelningen på en gång!

Om din mus flyttar på sig ”av sig själv” på skärmen kan det tyda på en allvarlig attack som involverar en dataläcka och kanske även loggning av tangenttryckningar. Din IT-avdelning måste få reda på det här på en gång för att kunna reda ut det.

Nästa fråga

DELL Technologies

SVAR

PC-infiltrering

Nr 5

HACKAD!!!

Kontakta IT-avdelningen på en gång!

Onormalt beteende kan tyda på att en angripare övervakar din PC och kanske både stjäl data och loggar tangenttryckningar, inklusive dina lösenord och annan viktig information. Det är bäst att stänga av din PC på en gång och rapportera problemet till din IT-avdelning.

Nästa fråga

DELL Technologies

FRÅGA 6 AV 14

USB-aktiverad attack med skadligt program

Du ser en plastpåse ligga mellan två bilar på företagets parkeringsplats. Du ser att den innehåller fem USB-minnen förseglade i originalförpackningen. 500 GB styck!

Vad gör du?

Nr 6

Välj det bästa svaret nedan

A Öppnar ett av dem och sätter det i USB-uttaget på din PC och ger de andra USB-minnena till dina kollegor.

B Tar med dem hem och använder dem på din personliga dator.

C Säger till byggnadens säkerhetsvakter och IT-avdelningen och ger USB-minnena till dem.

D Ger USB-minnena till dina barn i julklapp.

E Inga av dessa.

DELL Technologies

SVAR

USB-aktiverad attack med skadligt program

Nr 6

BRA JOBBAT!

Säg till säkerhetsvakterna och IT-avdelningen!

Med sådana här attacker kan angripare placera skadliga program i en organisation genom att använda en medarbetare för att infoga en skadlig nyttolast i nätverket. Sätt aldrig ett USB-minne eller andra tillbehör från okända källor i NÅGON enhet som du äger. Och de är jättedåliga presenter!

Nästa fråga

DELL Technologies

SVAR

USB-aktiverad attack med skadligt program

Nr 6

HACKAD!!!

Säg till säkerhetsvakterna och IT-avdelningen!

Med sådana här attacker kan angripare placera skadliga program i en organisation genom att använda en medarbetare för att infoga en skadlig nyttolast i nätverket. Sätt aldrig ett USB-minne eller andra tillbehör från okända källor i NÅGON enhet som du äger. Och de är jättedåliga presenter!

Nästa fråga

DELL Technologies

FRÅGA 7 AV 14

Ransomware

En försäljare kommer till kontoret för att ge en presentation om ny teknik som företaget funderar på att införskaffa. Hen har sin presentation på ett USB-minne och ber dig sätta det i din PC så att presentationen kan visas medan hen pratar.

Vad gör du?

Nr 7

Välj det bästa svaret nedan

A Gör som hen säger och sätter USB-minnet i din PC.

B Frågar om presentationen kan laddas ner i stället eftersom företagets policy inte tillåter att externa USB-minnen används, men när hen säger att hen inte kan ladda ner den gör du som hen säger och sätter USB-minnet i din PC.

C Ber hen genomföra presentationen utan bilder och sätter inte USB-minnet i din PC.

D Kontrollerar att hen inte hittade USB-minnet på en parkeringsplats och sätter det sedan i din PC.

E Kopierar USB-minnet och ger en kopia till din chef.

DELL Technologies

SVAR

Ransomware

Nr 7

BRA JOBBAT!

Visa inte upp och sätt inte i USB-minnet.

Du vet inte detta, men försäljaren har blivit mutad av en angripare och USB-minnet innehåller en ransomware-nyttolast som låser era system. Men genom att inte sätta USB-minnet i din PC och inte ladda ner några andra filer har du hindrat angriparen från att få åtkomst. Vilken tur!

Nästa fråga

DELL Technologies

SVAR

Ransomware

Nr 7

HACKAD!!!

Visa inte upp och sätt inte i USB-minnet.

Du vet inte detta, men försäljaren har blivit mutad av en angripare och USB-minnet och nedladdade filer innehåller en ransomwarenyttolast som låser era system. Undvik att använda externa USB-minnen och ladda inte ner filer från okända källor till personliga eller företagsägda datorer.

Nästa fråga

DELL Technologies

FRÅGA 8 AV 14

Tvåfaktorsautentisering

Din bank rekommenderar att du använder tvåfaktorsautentisering när du loggar in på deras webbplats. Andra webbplatser använder också denna process för att skydda användare.

Vad av följande är exempel på tvåfaktorsautentisering?

Nr 8

Välj det bästa svaret nedan

A	Du anger ditt användarnamn och lösenord och blir sedan ombedd att ange din PIN-kod för att få åtkomst till webbplatsen.
B	Du anger ditt användarnamn och lösenord, plus en CAPCHA där du väljer rutor med skyltar.
C	Du anger ditt användarnamn och lösenord och webbplatsen skickar ett sms till din mobil med en engångskod som du anger i rutan på webbplatsen.
D	Du anger ditt användarnamn och webbplatsen kräver att du anger en kod från en säkerhetstoken som ändras varje minut, som har installerats på din mobil.
E	Endast A och C.
F	Endast C och D.
G	Inga av dessa.

DELL Technologies

SVAR

Tvåfaktorsautentisering

Nr 8

BRA JOBBAT!

Du behöver båda två!

Med tvåfaktorsautentisering krävs både ett lösenord och en annan, annorlunda identifierare – såsom en kod som skickas via sms eller ett nummer som genereras av en app – för att identifiera och autentisera användare. Det här säkerhetslagret gör det mycket svårare för angripare att komma åt din information.

Nästa fråga

DELL Technologies

SVAR

Tvåfaktorsautentisering

Nr 8

BRA JOBBAT, MEN ...

Du behöver båda två!

Du hade nästan rätt! Det finns två exempel på tvåfaktorsautentisering här. Försök igen för att se om du kan upptäcka det andra exemplet också.

Nästa fråga

DELL Technologies

SVAR

Tvåfaktorsautentisering

Nr 8

HACKAD!!!

Hoppsan! Du behöver båda två!

Med tvåfaktorsautentisering krävs både ett lösenord och en annan, annorlunda identifierare – såsom en kod som skickas via sms eller ett nummer som genereras av en app – för att identifiera och autentisera användare. Det här säkerhetslagret gör det mycket svårare för angripare att komma åt din information. Om du inte använder det är du sårbar för attacker.

Nästa fråga

DELL Technologies

FRÅGA 9 AV 14

Bluetooth-tjuvar

Du kör till en fin vandringsled för en trevlig eftermiddag i naturen, men upptäcker att du har din bärbara dator i ryggsäcken och din mobil i fickan (som inte har täckning här). Du behöver lämna datorn och mobilen i bilen, men vill se till att de är säkra.

Vad gör du?

Nr 9

Välj det bästa svaret nedan

A Stänger av all Wi-Fi.

B Aktiverar datorns viloläge.

C Låser in datorn och mobilen i bagageutrymmet.

D Lindar in datorn och mobilen i en tjock filt.

E Stänger av datorn och mobilen helt, vilket inaktiverar Bluetooth.

DELL Technologies

SVAR

Bluetooth-tjuvar

Nr 9

BRA JOBBAT!

Stäng av datorn och mobilen!

Det är alltid bäst att lägga enheter utom synhåll när du lämnar dem i bilen, men tjuvar använder Bluetooth-skanners för att hitta enheter i låsta bilar, och alla enheter inaktiverar inte Bluetooth när de ”vilar”. Stölder inträffar ofta vid vandringsleder och på andra platser där ägarna kommer att vara borta ett tag, och tjuvarna håller alltid utkik! Så tänk på det innan du ger dig ut i naturen!

Nästa fråga

DELL Technologies

SVAR

Bluetooth-tjuvar

Nr 9

HACKAD!!!

Stäng av datorn och mobilen!

Det är alltid bäst att lägga enheter utom synhåll när du lämnar dem i bilen, men tjuvar använder Bluetooth-skanners för att hitta enheter i låsta bilar, och alla enheter inaktiverar inte Bluetooth när de ”vilar”. Stölder inträffar ofta vid vandringsleder, där ägarna kommer att vara borta ett tag, så tänk på det innan du ger dig ut i naturen!

Nästa fråga

DELL Technologies

FRÅGA 10 AV 14

USB-attack, del 2

Du vill skapa lite julstämning, så du tar med dig en liten USB-julgran till kontoret.

Hur driver du den?

Nr 10

Välj det bästa svaret nedan

A Du ansluter den till din PC.

B Du ansluter den till en USB-förlängare som är ansluten till din PC.

C Du använder en särskild USB-laddare för att ansluta julgranen till ett vanligt eluttag.

D Du kan inte ansluta den någonstans. Julen är inställd.

E Inga av dessa.

DELL Technologies

SVAR

USB-attack, del 2

Nr 10

BRA JOBBAT!

Använd en särskild USB-laddare!

I den här sortens USB-attack sätts skadliga program på massor av enheter, till och med små julgranar! Angriparna hoppas att de kommer att anslutas till värdefulla företagsnätverk. Anslut aldrig en okänd USB-enhet till din PC, inte ens för att ladda den.

Nästa fråga

DELL Technologies

SVAR

USB-attack, del 2

Nr 10

HACKAD!!!

Använd en särskild USB-laddare!

I den här sortens USB-attack sätts skadliga program på massor av enheter, till och med små julgranar! Angriparna hoppas att de kommer att anslutas till värdefulla företagsnätverk. Anslut aldrig en okänd USB-enhet till din PC, inte ens för att ladda den.

Nästa fråga

DELL Technologies

FRÅGA 11 AV 14

Den onda städerskan

Du är på en cybersäkerhetskonferens i Shanghai i Kina och bor på ett femstjärnigt hotell. Innan du går ut på middag låser du in din PC i kassaskåpet i ditt rum.

Är datorn skyddad från attacker och stöld?

Nr 11

Välj det bästa svaret nedan

A Nej, för alla enheter som lämnas obevakade kan attackeras.

B Ja, för den är inlåst i kassaskåpet.

C Ja, för du hängde kläder framför kassaskåpet i garderoben.

D Ja, för det är ett lyxigt hotell.

E Ja, för det är inte en särskilt bra PC.

DELL Technologies

SVAR

Den onda städerskan

Nr 11

BRA JOBBAT!

Nej, alla enheter kan attackeras!

Alla enheter som lämnas obevakade kan öppnas och komprometteras med en så kallad ”Evil Maid”-attack (ond städerska), där angriparen får fysisk åtkomst till datorn och infogar ett skadligt program. Om du inte har enheten hos dig kan den attackeras. Och låt aldrig någon du inte känner ta hand om din enhet, särskilt inte om det är en ond städerska.

Nästa fråga

DELL Technologies

SVAR

Den onda städerskan

Nr 11

HACKAD!!!

Nej, alla enheter kan attackeras!

Alla enheter som lämnas obevakade kan öppnas och komprometteras med en så kallad ”Evil Maid”-attack (ond städerska), där angriparen får fysisk åtkomst till datorn och infogar ett skadligt program. För säkerhets skull måste du ha dina enheter hos dig. Låt aldrig någon du inte känner ta hand om din enhet, särskilt inte om det är en ond städerska.

Nästa fråga

DELL Technologies

FRÅGA 12 AV 14

Spionprogram

Du får ett sms från ett nummer som du tror att du känner igen, där det står att din dotter har varit med om en olycka och har tagits till sjukhuset. Meddelandet innehåller en länk så att du kan kontakta sjukhuset.

Vad gör du?

Nr 12

Välj det bästa svaret nedan

A	Du klickar genast på länken eftersom du är orolig för din dotter.
B	Du kollar upp numret, ser att det är från området där din dotter var och klickar på länken.
C	Du klickar inte på länken utan sms:ar i stället din dotter för att kolla att hon är okej.
D	Inga av dessa.

DELL Technologies

SVAR

Spionprogram

Nr 12

BRA JOBBAT!

Klicka inte på länken!

Sådana här attacker är försök att placera spionprogram på din mobil, vilket kan kompromettera mobilen och kanske spridas till företagets nätverk. Du märkte att något verkade misstänkt och använde en annan metod för att kolla att din dotter var okej.

Bra jobbat!

Nästa fråga

DELL Technologies

SVAR

Spionprogram

Nr 12

HACKAD!!!

Klicka inte på länken!

Sådana här attacker är försök att placera spionprogram på din mobil, vilket kan kompromettera mobilen och kanske spridas till företagets nätverk. Om du klickar på länken installeras en nyttolast med spionprogram på din enhet. Ignorera oväntade sms från okända avsändare, oavsett hur övertygande de är.

Nästa fråga

DELL Technologies

FRÅGA 13 AV 14

Slutpunktssäkerhet

Hotaktörer (man kan till och med kalla dem hackare med skadligt uppsåt) attackerar slutpunkter.

Exempel på slutpunkter:

Nr 13

Välj det bästa svaret nedan

A	Stationära datorer.
B	Stationära och bärbara datorer.
C	Stationära och bärbara datorer och servrar.
D	Stationära och bärbara datorer, servrar, molnet med mera.
E	Stationära och bärbara datorer, servrar, molnet och den senaste destinationen på min GPS.

DELL Technologies

SVAR

Slutpunktssäkerhet

Nr 13

BRA JOBBAT!

Alla fjärranslutna enheter!

En slutpunkt är en enhet som är fjärransluten till ett nätverk. Slutpunktssäkerhet är avgörande för att skydda enheter och data inom organisationen, så se till att ligga steget före angripare!

Nästa fråga

DELL Technologies

SVAR

Slutpunktssäkerhet

Nr 13

BRA JOBBAT, MEN ...

Alla fjärranslutna enheter!

En slutpunkt är en enhet som är fjärransluten till ett nätverk. Slutpunktssäkerhet är avgörande för att skydda enheter och data inom organisationen, så se till att ligga steget före angripare!

Nästa fråga

DELL Technologies

SVAR

Slutpunktssäkerhet

Nr 13

HACKAD!!!

Alla fjärranslutna enheter!

En slutpunkt är en enhet som är fjärransluten till ett nätverk. Slutpunktssäkerhet är avgörande för att skydda enheter och data inom organisationen, så se till att ligga steget före angripare!

Nästa fråga

DELL Technologies

FRÅGA 14 AV 14

Slutpunktssäkerhet, del 2

Hackare med skadligt uppsåt attackerar slutpunkter såsom stationära och bärbara datorer, mobiler, trådlösa skrivare, servrar … Allt som ansluts till ett nätverk.

Vad bör du göra för att förhindra en attack?

Nr 14

Välj det bästa svaret nedan

A Se till att jag låser, och låser in, min enhet när jag inte använder den.

B Uppdatera och installera korrigeringsfiler på min enhet regelbundet.

C Ha god e-posthygien: Rapportera misstänkta meddelanden.

D Aldrig ansluta en okänd enhet till min slutpunkt.

E Alla dessa.

DELL Technologies

SVAR

Slutpunktssäkerhet, del 2

Nr 14

BRA JOBBAT!

Alla dessa!

Du har lärt dig att vara cybersäker och använder dessa rutiner i praktiken. Slutpunktssäkerhet är avgörande för att skydda enheter och data inom organisationen, så se till att ligga steget före angripare!

Nästa fråga

DELL Technologies

SVAR

Slutpunktssäkerhet, del 2

Nr 14

BRA JOBBAT, MEN ...

Det finns mer att göra!

Du måste göra mer än en sak för att skydda dina enheter. Slutpunktssäkerhet är avgörande för att skydda enheter och data inom organisationen, så se till att ligga steget före angripare!

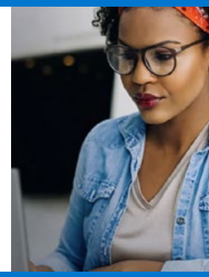
Nästa fråga

DELL Technologies

TACK!

Det finns mer information

på **Dell.com/Endpoint-Security**



DELL Technologies