DELL Technologies

Você sabe mais do que seu cyber attacker?

Iniciar o teste

PERGUNTA 1 DE 14

Phishing

Você recebe um e-mail de "Pedido do Windows Defender" com uma fatura que parece oficial de US$ 399,99 para uma assinatura de um ano na conta do Microsoft Defender. Afirma claramente "Não responda a este e-mail", mas indica um botão de "Ajuda e contato" com um número de telefone. Você não se lembra de ter feito esse pedido.

O que fazer?

Nº 1

Selecione a melhor resposta abaixo

A Clica imediatamente no botão "Ajuda e contato", pois definitivamente não quer que essa cobrança seja feita no cartão de crédito!

B Abre o e-mail em uma janela anônima do navegador da Web e clica no botão "Ajuda e contato".

C Verifica o extrato do cartão de crédito on-line para ver se a cobrança foi realizada e usa o número de telefone para tentar descobrir mais informações.

D Inspeciona o endereço de e-mail e percebe que parece phishing, então clica em "Denunciar phishing" por meio do seu programa de e-mail e/ou o encaminha ao seu departamento de TI para investigação – e é claro, não o abre!

E Exclui o e-mail sem abri-lo.

DELL Technologies

RESPOSTA

Phishing

Nº 1

MUITO BEM!

Denuncie phishing!

Ao receber um e-mail suspeito solicitando que clique em links por qualquer motivo, a melhor ação é excluir o e-mail sem abri-lo ou clicar em "Denunciar phishing" na barra do Outlook para denunciá-lo à TI para investigação. **Se parece phishing, provavelmente é.**

Próxima pergunta

DELL Technologies

RESPOSTA

Phishing

Nº 1

MUITO BEM, MAS...

Denuncie phishing!

Você ainda se coloca em risco ao ligar para o que será um número de telefone falso. Uma das outras opções nesta lista é uma solução melhor. **Se parece phishing, provavelmente é.**

Próxima pergunta

DELL Technologies

RESPOSTA

Phishing

Nº 1

HACKEADO!!!

Denuncie phishing!

Lembre-se: ao receber um e-mail suspeito solicitando que clique em links por qualquer motivo, a melhor ação é excluir o e-mail sem abri-lo ou clicar em "Denunciar phishing" na barra do Outlook para denunciá-lo à TI para investigação.

Se parece phishing, provavelmente é.

Próxima pergunta

DELL Technologies

PERGUNTA 2 DE 14

Phishing de mídia social

Você acessa sua conta do Instagram e vê que Lyle Lovett respondeu diretamente ao seu comentário nas postagens dele! Ele pede para que você o siga por meio de uma mensagem via direct e envia um link para que você clique e acesse um conteúdo muito exclusivo e valioso.

Você:

Nº 2

Selecione a melhor resposta abaixo

A Mal pode acreditar na sorte que tem e clica imediatamente no link.

B Copia o link e o abre em uma janela anônima.

C Compartilha o link nas mídias sociais com seus amigos.

D Posiciona o cursor do mouse sobre o link e suspeita que seja phishing, então exclui a mensagem e bloqueia o remetente.

E Bloqueia e denuncia o remetente sem clicar em nada.

DELL Technologies

RESPOSTA

Phishing de mídia social

Nº 2

MUITO BEM!

Denuncie phishing!

Ao receber um e-mail suspeito solicitando que clique em links por qualquer motivo, a melhor ação é excluir o e-mail sem abri-lo ou clicar em "Denunciar phishing" na barra do Outlook para denunciá-lo à TI para investigação. **Se parece phishing, provavelmente é.**

Próxima pergunta

DELL Technologies

RESPOSTA

Phishing de mídia social

Nº 2

HACKEADO!!!

Denuncie phishing!

Lembre-se: ao receber um e-mail suspeito solicitando que clique em links por qualquer motivo, a melhor ação é excluir o e-mail sem abri-lo ou clicar em "Denunciar phishing" na barra do Outlook para denunciá-lo à TI para investigação.

Se parece phishing, provavelmente é.

Próxima pergunta

DELL Technologies

PERGUNTA 3 DE 14

Segurança da senha

O departamento de TI incentiva criar senhas complexas – isso porque essas "credenciais" estão entre os alvos mais procurados pelos invasores. Então...

Como deixar a senha mais segura?

Nº 3

Selecione a melhor resposta abaixo

A	Criar uma senha longa com pelo menos 8 caracteres.
B	Usar uma combinação de letras, números e caracteres.
C	Evitar reutilizar qualquer uma das senhas em contas ou sites (criar senhas únicas).
D	Todas as alternativas acima.
E	Nenhuma das alternativas acima.

DELL Technologies

RESPOSTA

Segurança da senha

Nº 3

MUITO BEM!

Use uma senha complexa!

Uma senha segura é única e combina pelo menos oito letras, números e caracteres – e talvez até use uma frase secreta exclusiva que você lembre. E não use o nome do seu cachorro! Além disso, use a autenticação de dois fatores. Ela, além da senha complexa, dá a proteção ideal.

Próxima pergunta

DELL Technologies

RESPOSTA

Segurança da senha

Nº 3

MUITO BEM, MAS...

Use uma senha complexa!

Uma senha segura combina todas as medidas de segurança listadas: é única e contém pelo menos oito letras, números e caracteres. E não use o nome do seu cachorro! Para reforçar a segurança, use a autenticação de dois fatores e frases secretas com números e caracteres em vez de senhas.

Próxima pergunta

DELL Technologies

RESPOSTA

Segurança da senha

Nº 3

HACKEADO!!!

Use uma senha complexa!

Uma senha segura é única e combina pelo menos oito letras, números e caracteres. Para reforçar a segurança, use a autenticação de dois fatores e frases secretas com números e caracteres em vez de senhas.

Próxima pergunta

DELL Technologies

PERGUNTA 4 DE 14

Engenharia social

Você recebe em seu celular uma ligação de alguém que alega ser do departamento de TI informando que a senha expirou e você precisa criar uma nova. O número de telefone parece seguro. A pessoa pede para que você dê seu número de funcionário, CPF e data de nascimento para verificação.

O que fazer?

Nº 4

Selecione a melhor resposta abaixo

A Dá as informações, pois quer trocar a senha e voltar ao trabalho.

B Pede o e-mail de contato e o número de telefone da pessoa para confirmar a identidade dela e passa as informações solicitadas.

C Encerra a chamada imediatamente e informa o caso ao departamento de TI.

D Informa o número de funcionário e a data de nascimento, menos o CPF.

E Nenhuma das alternativas acima.

DELL Technologies

RESPOSTA

Engenharia social

Nº 4

MUITO BEM!

Encerre a chamada e entre em contato com a TI!

Alguns invasores usam a engenharia social para induzir que você passe informações confidenciais por telefone. Mesmo que você consiga confirmar no sistema que as informações passadas pertencem a um funcionário, não há garantia de que esteja realmente falando com a pessoa certa. **Trocas de senha devem sempre ser iniciadas por você.**

Próxima pergunta

DELL Technologies

RESPOSTA

Engenharia social

Nº 4

HACKEADO!!!

Encerre a chamada e entre em contato com a TI!

Alguns invasores usam a engenharia social para induzir que você passe informações confidenciais por telefone. Mesmo que você consiga confirmar no sistema que as informações passadas pertencem a um funcionário, não há garantia de que esteja realmente falando com a pessoa certa. **Trocas de senha devem sempre ser iniciadas por você.**

Próxima pergunta

DELL Technologies

PERGUNTA 5 DE 14

Invasão no PC

Ao atender uma chamada, você percebe um comportamento estranho na tela, como o mouse se movendo sozinho, texto ou janelas do console abrindo e fechando ou menus aparecendo de repente.

Então:

Nº 5

Selecione a melhor resposta abaixo

A Você acha que é um problema inofensivo no PC e continua trabalhando.

B Você fala com o departamento de TI sobre isso, mas continua trabalhando.

C Imediatamente para de usar o PC, desliga-o e entra em contato com o departamento de TI (usando outro dispositivo) para comunicar o problema.

DELL Technologies

RESPOSTA

Invasão no PC

Nº 5

MUITO BEM!

Entre em contato com a TI imediatamente!

O mouse se movendo "sozinho" na tela pode indicar um ataque sério envolvendo violação de dados e possível registro de teclas pressionadas. O departamento de TI precisa saber disso o mais rápido possível para fazer um acompanhamento eficaz.

Próxima pergunta

DELL Technologies

RESPOSTA

Invasão no PC

Nº 5

HACKEADO!!!

Entre em contato com a TI imediatamente!

O comportamento anormal pode indicar que um invasor está monitorando o PC e pode estar fazendo a exfiltração de dados e o registro das teclas pressionadas, como senhas e outras informações críticas. A melhor opção é desligar o PC imediatamente e comunicar o problema ao departamento de TI.

Próxima pergunta

DELL Technologies

PERGUNTA 6 DE 14

Ataque de malware via pen drive

Ao caminhar pelo estacionamento da sua empresa, você vê uma sacola de compras entre dois carros. Você percebe que ela contém cinco pen drives ainda lacrados na embalagem original – 500 GB cada!

O que fazer?

Nº 6

Selecione a melhor resposta abaixo

A Abre um, conecta-o à entrada USB do PC e dá os outros exemplares aos colegas de trabalho.

B Leva os pen drives para casa e usa-os no computador pessoal.

C Notifica as equipes de segurança do prédio e do departamento de TI sobre a descoberta e entrega-lhes os pen drives.

D Dá os pen drives de presente aos seus filhos no Natal.

E Nenhuma das alternativas acima.

DELL Technologies

RESPOSTA

Ataque de malware via pen drive

Nº 6

MUITO BEM!

Notifique a segurança e a TI!

Esse tipo de ataque permite que um invasor instale malwares em uma organização usando um funcionário como "mula" para inserir o payload mal-intencionado na rede. Nunca insira pen drives ou outros acessórios de fontes desconhecidas em NENHUM dispositivo seu. E esses são presentes terríveis!

Próxima pergunta

DELL Technologies

RESPOSTA

Ataque de malware via pen drive

Nº 6

HACKEADO!!!

Notifique a segurança e a TI!

Esse tipo de ataque permite que um invasor instale malwares em uma organização usando um funcionário como "mula" para inserir o payload mal-intencionado na rede. Nunca insira pen drives ou outros acessórios de fontes desconhecidas em NENHUM dispositivo seu. E esses são presentes terríveis!

Próxima pergunta

DELL Technologies

PERGUNTA 7 DE 14

Ransomware

Um vendedor vai até o escritório para fazer uma apresentação sobre uma tecnologia nova que a empresa está interessada em comprar. Leva a apresentação em um pen drive e pede que você o insira no PC para que ela seja projetada enquanto ele fala sobre a tecnologia.

O que fazer?

Nº 7

Selecione a melhor resposta abaixo

A Faz o que foi pedido e conecta o pen drive ao PC.

B Pergunta se é possível fazer download da apresentação, pois a política da empresa proíbe o uso de unidades USB externas, porém, quando o download não é possível, você faz o que foi pedido e conecta o pen drive ao PC.

C Pede para que a apresentação seja realizada sem utilizar projeção e não conecta o pen drive.

D Confirma se o pen drive não foi encontrado em um estacionamento e conecta-o ao PC.

E Faz outras cópias do pen drive e dá uma ao gerente.

DELL Technologies

RESPOSTA

Ransomware

Nº 7

MUITO BEM!

Não realize a projeção nem conecte o pen drive.

Sem o seu conhecimento, o vendedor recebeu uma boa quantia de um invasor e o pen drive contém um payload com ransomware que bloqueará os sistemas: mas ao não conectar o pen drive e não realizar o download de nenhum outro arquivo, você impediu o acesso do invasor. Ufa!

Próxima pergunta

DELL Technologies

RESPOSTA

Ransomware

Nº 7

HACKEADO!!!

Não realize a projeção nem insira o pen drive.

Sem o seu conhecimento, o vendedor recebeu uma boa quantia de um invasor e o pen drive contém um payload com ransomware que bloqueará os sistemas. Evite utilizar pen drives externos e fazer o download de arquivos de fontes desconhecidas em computadores pessoais ou PCs da empresa.

Próxima pergunta

DELL Technologies

PERGUNTA 8 DE 14

Autenticação de dois fatores

Seu banco recomendou que você utilize a autenticação de dois fatores ao fazer log-in no site dele. Outros sites também usam esse processo para garantir a segurança dos usuários.

Qual destes é um exemplo de autenticação de dois fatores?

Nº 8

Selecione a melhor resposta abaixo

A Você digita seu nome de usuário e senha e, aí recebe uma solicitação para inserir seu PIN a fim de ter acesso ao site.

B Você digita seu nome de usuário e senha, seguido de um CAPCHA em que você seleciona os painéis que incluem sinais.

C Você digita seu nome de usuário e senha e o site envia uma mensagem de texto para o seu celular com um código de utilização única que você insere no local fornecido no site.

D Você digita seu nome de usuário e o site exige que você insira um código de um token seguro que muda a cada minuto e é instalado em seu telefone.

E Alternativas A e C.

F Alternativas C e D.

G Nenhuma das alternativas acima.

DELL Technologies

RESPOSTA

Autenticação de dois fatores

Nº 8

MUITO BEM!

Você precisa dos dois!

A autenticação de dois fatores requer uma senha e um identificador adicional diferenciado - como um código enviado por texto ou um número gerado por um aplicativo - para identificar e autenticar usuários. Essa camada de segurança dificulta ainda mais o acesso dos invasores às suas informações.

Próxima pergunta

DELL Technologies

RESPOSTA

Autenticação de dois fatores

Nº 8

MUITO BEM, MAS...

Você precisa dos dois!

Você chegou perto! Há dois exemplos de autenticação de dois fatores aqui – tente novamente e veja se você consegue identificar o outro.

Próxima pergunta

DELL Technologies

RESPOSTA

Autenticação de dois fatores

Nº 8

HACKEADO!!!

Opa! Você precisa dos dois!

A autenticação de dois fatores requer uma senha e um identificador adicional diferenciado - como um código enviado por texto ou um número gerado por um aplicativo - para identificar e autenticar usuários. Essa camada de segurança dificulta ainda mais o acesso dos invasores às suas informações. Você ficará vulnerável a invasores se não a usar.

Próxima pergunta

DELL Technologies

PERGUNTA 9 DE 14

Roubo via Bluetooth

Depois de dirigir até uma trilha para uma boa tarde de caminhada, você descobre que seu notebook ainda está em sua mochila, além disso, você está com seu telefone (que está fora de área). Você precisa deixar seu computador e telefone no carro, mas quer fazer isso com segurança.

O que fazer?

Nº 9

Selecione a melhor resposta abaixo

A Desliga o Wi-Fi dos dispositivos.

B Coloca seu notebook no modo de suspensão.

C Guarda seu notebook e telefone no porta-malas.

D Envolve seu notebook e telefone em um cobertor grosso.

E Desliga seu notebook e o telefone completamente, o que desativa o Bluetooth.

DELL Technologies

RESPOSTA

Roubo via Bluetooth

Nº 9

MUITO BEM!

Desligue seu notebook e telefone!

Embora seja sempre melhor manter seus dispositivos fora de vista quando você não estiver com eles, os hackers estão usando scanners Bluetooth para localizar dispositivos em veículos fechados à chave – e nem todos os dispositivos desligam o Bluetooth quando estão no modo de suspensão. Os roubos geralmente ocorrem em trilhas e outros locais onde os proprietários dos dispositivos ficam ausentes por longos períodos – e os hackers estão sempre observando! Por isso, esteja atento antes de fazer caminhadas!

Próxima pergunta

DELL Technologies

RESPOSTA

Roubo via Bluetooth

Nº 9

HACKEADO!!!

Desligue seu notebook e telefone!

Embora seja sempre melhor manter seus dispositivos fora de vista quando você não estiver com eles, os hackers estão usando scanners Bluetooth para localizar dispositivos em veículos fechados à chave – e nem todos os dispositivos desligam o Bluetooth quando estão no modo de suspensão. Os roubos geralmente ocorrem em trilhas onde os proprietários dos dispositivos ficam ausentes por longos períodos – por isso, esteja atento antes de fazer caminhadas!

Próxima pergunta

DELL Technologies

PERGUNTA 10 DE 14

Ataque via USB - Parte 2

Em clima de festas, você traz uma mini árvore de Natal alimentada via USB para decorar o seu escritório.

De que forma você a liga?

Nº 10

Selecione a melhor resposta abaixo

A Conectando-a ao PC.

B Por meio de um extensor USB que se conecta ao PC.

C Usando um carregador USB dedicado para conectar o dispositivo a uma tomada comum.

D Não há como ligá-la, o Natal está cancelado.

E Nenhuma das alternativas acima.

DELL Technologies

RESPOSTA

Ataque via USB - Parte 2

Nº 10

MUITO BEM!

Use um carregador USB dedicado!

Esta variante de ataque via USB instala malwares em muitos dispositivos – até mesmo pequenas árvores de Natal! – na esperança de que elas acabem conectadas a uma valiosa rede corporativa. Nunca conecte um dispositivo USB desconhecido ao seu PC, mesmo que seja apenas para carregá-lo.

Próxima pergunta

DELL Technologies

RESPOSTA

Ataque via USB - Parte 2

Nº 10

HACKEADO!!!

Use um carregador USB dedicado!

Esta variante de ataque via USB instala malwares em muitos dispositivos – até mesmo pequenas árvores de Natal! – na esperança de que eles acabem conectados a uma valiosa rede corporativa. Nunca conecte um dispositivo USB desconhecido ao seu PC, mesmo que seja apenas para carregá-lo.

Próxima pergunta

DELL Technologies

PERGUNTA 11 DE 14

Ataque Evil Maid

Você está em uma conferência de segurança cibernética em Xangai, China, hospedado em um hotel 5 estrelas. Antes de sair para jantar, você tranca seu PC no cofre do seu quarto.

O PC está protegido contra ataques e roubos?

Nº 11

Selecione a melhor resposta abaixo

A	Não, pois qualquer dispositivo deixado sem supervisão pode ser violado.
B	Sim, pois você o trancou com segurança no cofre.
C	Sim, pois você também pendurou roupas no armário para esconder o cofre.
D	Sim, pois é realmente ótimo o hotel.
E	Sim, pois não é um PC muito bom.

DELL Technologies

RESPOSTA

Ataque Evil Maid

Nº 11

MUITO BEM!

Não, qualquer dispositivo pode ser violado!

Qualquer dispositivo deixado sem supervisão pode ser aberto e violado por meio do que é geralmente conhecido como ataque "Evil Maid", no qual um invasor consegue acessar o PC abrindo-o fisicamente para inserir o malware. Um dispositivo que não está fisicamente com você pode ser atacado. Além disso, nunca deixe seu dispositivo com uma pessoa desconhecida, especialmente se ela for uma camareira mal-intencionada (Evil Maid).

Próxima pergunta

DELL Technologies

RESPOSTA

Ataque Evil Maid

Nº 11

HACKEADO!!!

Não, qualquer dispositivo pode ser violado!

Qualquer dispositivo deixado sem supervisão pode ser aberto e violado por meio do que é geralmente conhecido como ataque "Evil Maid", no qual um invasor consegue acessar o PC abrindo-o fisicamente para inserir o malware. Para estar seguro, o dispositivo precisa estar com você. Nunca deixe seu dispositivo com uma pessoa desconhecida, especialmente se ela for uma camareira mal-intencionada (Evil Maid).

Próxima pergunta

DELL Technologies

PERGUNTA 12 DE 14

Spyware

Você recebe uma mensagem de texto de um número vagamente familiar dizendo que sua filha sofreu um acidente e foi levada para o hospital. Nela há um link para que você entre em contato imediatamente.

Você:

Nº 12

Selecione a melhor resposta abaixo

A	Clica imediatamente no link, pois está preocupado com sua filha.
B	Verifica o número, descobre que é da área onde sua filha estava e clica no link.
C	Não clica no link e, em vez disso, envia uma mensagem de texto para sua filha para ter certeza de que ela está bem.
D	Nenhuma das alternativas acima.

DELL Technologies

RESPOSTA

Spyware

Nº 12

MUITO BEM!

Não clique no link!

Esse tipo de ataque é uma tentativa de instalar um spyware em seu telefone, que pode comprometer seu telefone e possivelmente se espalhar pela rede corporativa. Você suspeitou que algo não parecia "certo" e usou outro método para verificar se sua filha estava bem.

Excelente!

Próxima pergunta

DELL Technologies

RESPOSTA

Spyware

Nº 12

HACKEADO!!!

Não clique no link!

Esse tipo de ataque é uma tentativa de instalar um spyware em seu telefone, que pode comprometer seu telefone e possivelmente se espalhar pela rede corporativa. Ao clicar no link, um payload de spyware é entregue ao seu dispositivo. Tenha cuidado com textos vagos, não importa o quão atrativos possam ser.

Próxima pergunta

DELL Technologies

PERGUNTA 13 DE 14

Segurança de endpoint

Agentes mal-intencionados (você pode até chamá-los de hackers mal-intencionados) estão de olho nos endpoints.

Endpoints são definidos como:

Nº 13

Selecione a melhor resposta abaixo

A	Desktops.
B	Desktops e notebooks.
C	Desktops, notebooks e servidores.
D	Desktops, notebooks, servidores, nuvem e muito mais.
E	Desktops, notebooks, servidores, nuvem e o último destino em meu GPS.

DELL Technologies

RESPOSTA

Segurança de endpoint

Nº 13

MUITO BEM!

Qualquer dispositivo conectado remotamente!

Um endpoint é qualquer dispositivo conectado remotamente a uma rede. A segurança do endpoint é essencial para proteger os dispositivos e os dados em sua organização, portanto, esteja à frente dos invasores!

Próxima pergunta

DELL Technologies

RESPOSTA

Segurança de endpoint

Nº 13

MUITO BEM, MAS...

Qualquer dispositivo conectado remotamente!

Um endpoint é qualquer dispositivo conectado remotamente a uma rede. A segurança do endpoint é essencial para proteger os dispositivos e os dados em sua organização, portanto, esteja à frente dos invasores!

Próxima pergunta

DELL Technologies

RESPOSTA

Segurança de endpoint

Nº 13

HACKEADO!!!

Qualquer dispositivo conectado remotamente!

Um endpoint é qualquer dispositivo conectado remotamente a uma rede. A segurança do endpoint é essencial para proteger os dispositivos e os dados em sua organização, portanto, esteja à frente dos invasores!

Próxima pergunta

DELL Technologies

PERGUNTA 14 DE 14

Segurança de endpoint - Parte 2

Hackers mal-intencionados visam endpoints como desktops, notebooks, telefones celulares, impressoras sem fio, servidores – qualquer coisa que se conecte a uma rede.

O que você deve fazer para ajudar a evitar um ataque?

Nº 14

Selecione a melhor resposta abaixo

A	Ter a certeza de que o meu dispositivo está bloqueado - e bloqueá-lo - sempre que ele não estiver sendo utilizado.
B	Atualizar e instalar Patchs em meu dispositivo regularmente.
C	Realizar uma boa higiene de e-mail: denunciar e-mails suspeitos.
D	Nunca conectar um dispositivo desconhecido ao meu endpoint.
E	Todas as alternativas acima.

DELL Technologies

RESPOSTA

Segurança de endpoint - Parte 2

Nº 14

MUITO BEM!

Todas as alternativas acima!

Você aprendeu sobre como se proteger no mundo virtual e está colocando isso em prática. A segurança do endpoint é essencial para proteger os dispositivos e os dados em sua organização, portanto, esteja à frente dos invasores!

Próxima pergunta

DELL Technologies

RESPOSTA

Segurança de endpoint - Parte 2

Nº 14

MUITO BEM, MAS...

Há mais a fazer!

Há mais do que uma opção a ser feita para proteger seus dispositivos. A segurança do endpoint é essencial para proteger os dispositivos e os dados em sua organização, portanto, esteja à frente dos invasores!

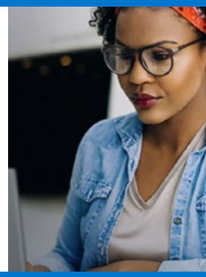
Próxima pergunta

DELL Technologies

OBRIGADO!

Para obter mais informações:

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



DELL Technologies