

Descubra agora o quanto você está preparado para se manter seguro na Internet enquanto trabalha e como proteger os dados de sua empresa (e de seus clientes).

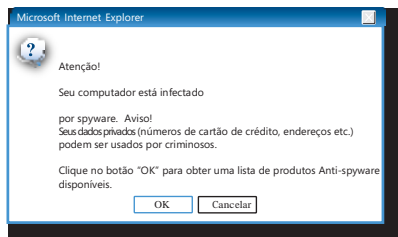
1. Quais das senhas a seguir podem ser consideradas senhas fortes? (Selecione todas as corretas.)


- T3cn0l0g!a
- Ch0ckL!ck
- O nome do seu animal de estimação
- 011235813
- A primeira letra de cada palavra em um ditado, frase ou outra sentença que, para você, seja fácil de lembrar.

2. Tudo bem se você compartilhar sua senha com: (Selecione as opções corretas.)

- Seu chefe
- Seu cônjuge
- O gerente do hotel
- Seus colegas de trabalho
- Recursos Humanos
- Nenhuma das alternativas acima

3. Se você perceber uma janela pop-up como esta quando estiver na Web, você deve:



- (a) Clicar em **OK** para decidir se é uma oferta legítima.
- (b) Clicar em **Cancelar**.
- (c) Pressione ALT + F4 para fechar a janela.
- (d) Clicar no botão .

4. Se você estiver usando uma rede Wi-Fi pública (em um café ou hotel, por exemplo) que fornece uma senha, suas comunicações estarão seguras.

- (a) Verdadeiro
- (b) Falso

5. Como você pode proteger seus dados quando estiver fora de casa ou escritório?

- (a) Bloquear o seu laptop e seu telefone celular com senhas.
- (b) Não levar dados confidenciais para fora do escritório. (Se necessário, você deve criptografá-los)
- (c) Certifique-se de que a conexão Wi-Fi pública criptografa os dados.
- (d) Todas as alternativas acima.

6. Faça uma lista com três sinais de fraude em um email ou mensagens instantâneas:

- 1. _____
- 2. _____
- 3. _____

7. Se você receber um email ou uma mensagem instantânea de um gerente de sua empresa, pedindo informações pessoais confidenciais (como uma senha ou o seu número de CPF), não há problema se você fornecer esses dados.

- (a) Verdadeiro
- (b) Falso

8. Quando um email ou mensagem instantânea vier com anexos e links, a sua melhor opção é: (Selecione todas as corretas.)

- Olhar todos com suspeita.
- Se a mensagem vier de alguém que você conhece pessoalmente, abra ou clique no anexo.
- Se a mensagem vier de uma fonte em que você confia, como a empresa em que você trabalha regularmente, abra ou clique nele.
- Não abra ou clique no anexo se ele estiver fora de contexto – por exemplo, *coelhinhos&unicórnios.bmp* vindo de seu chefe.
- Verifique o link ou anexo para então decidir se eles são seguros para se clicar.

9. Se você instalou todas as atualizações de segurança solicitadas pelo TI, você ainda deve se preocupar com vírus quando clicar em links ou abrir arquivos anexos em emails ou mensagens instantâneas.

- (a) Verdadeiro
- (b) Falso

10. Quais das seguintes extensões de arquivos anexados podem conter vírus e devem ser vistas como suspeitas?

- .exe
- .vsb
- .scr
- .pdf
- Todas as alternativas acima.

Respostas

1. Certas:

- Ch0ckL!ck: Esta é uma palavra pronunciada errada por uma criança, portanto não está em dicionário algum; ela usa letras maiúsculas e minúsculas, números e símbolos.
- A primeira letra de cada palavra de uma sentença que para você seja fácil de lembrar, uma linha de seu poema preferido, um ditado popular etc. É fácil para você lembrar, mas difícil para os outros adivinharem.

Erradas:

- T3cn0l0g!a: Os criminosos não serão tapeados por substituições visualmente semelhantes de letras em palavras que existam no dicionário.
- O nome do seu animal de estimação.
- 011235813: Evite sequências numéricas. (Esta é da série Fibonacci.)

2. Nenhuma das alternativas acima. Trate suas senhas com muita cautela assim como as informações que elas protegem.

3. (c) Qualquer item selecionável em uma janela pop-up – até mesmo o botão de Fechar do Windows – pode estar programado para baixar softwares maliciosos.

4. Falso. A senha simplesmente significa que apenas aqueles com uma senha podem acessar às suas comunicações. A próxima etapa é ter certeza de que o ponto de acesso sem fio criptografe seus dados.

5. (d)

6. As respostas podem incluir:

- Você ganhou um sorteio para o qual nunca se inscreveu. Alguém lhe pagará uma grande quantia em dinheiro como pagamento por sua ajuda na transferência de fundos.
- Erros ortográficos, erros gramaticais, formatação incomum.
- Alertas urgentes de empresas de sua confiança ou de alguém na sua empresa para evitar o fechamento de sua conta, para verificar sua conta, para atualizar bancos de dados, etc.

7. Falso. É possível que alguém tenha invadido a rede da empresa e esteja mandando emails diretamente da conta do gerente. Para verificar a autenticidade da solicitação, ligue para o seu gerente usando um número de telefone que você tenha em seu celular ou agenda e não um que esteja nas mensagens de email ou IM.

8. Certas:

- Olhar todos com suspeita.
- Não abra ou clique no anexo se ele estiver fora de contexto.

9. Verdadeiro. Alguém poderia invadir a rede da empresa e estaria mandando emails em nome do gerente.

10. Todas as alternativas acima. Qualquer arquivo anexado pode servir de meio de transporte para um vírus.

