SEGURANÇA PARA NAVEGAR PELA *INTERNET*

01. Por que os navegadores não protegem você de todas as ameaças cibernéticas?
a) Porque os navegadores não têm recursos de segurança.
b) Porque os navegadores não conseguem detectar todas as ameaças cibernéticas.
c) Porque os cibercriminosos são mais inteligentes que os navegadores.
d) Porque os navegadores são vulneráveis a ataques cibernéticos.

02. O que os cibercriminosos buscam ao criar sites falsos?
a) Credenciais de acesso do usuário.
b) Detalhes de cartão de crédito do usuário.
c) Contatos de redes sociais do usuário.
d) Todas as opções anteriores.

03. Como os usuários podem se proteger contra sites falsos?
a) Não clicando em links suspeitos ou desconhecidos.
b) Verificando se o site é legítimo antes de inserir informações pessoais ou financeiras.
c) Usando navegadores que possuem recursos de segurança avançados.
d) Todas as opções anteriores.

04. O que é um erro básico e perigoso no que se refere a senhas?
a) Utilizar senhas curtas.
b) Utilizar senhas fáceis de adivinhar.
c) Utilizar as mesmas combinações de senha em todos os aplicativos, serviços e sites.
d) Todas as opções anteriores.

05. Qual é a recomendação ideal para criar senhas seguras?
a) Utilizar apenas letras minúsculas em todas as senhas.
b) Utilizar senhas com menos de oito caracteres para facilitar a memorização.
c) Utilizar senhas com oito ou mais caracteres, combinando letras maiúsculas, minúsculas, números e símbolos.
d) Utilizar senhas fáceis de adivinhar para não esquecer.

06. Por que é importante manter os programas atualizados?
a) Para ter novos recursos e funcionalidades.
b) Para melhorar o desempenho do computador.
c) Para corrigir falhas e vulnerabilidades de segurança.
d) Para economizar dinheiro.

07. O que são updates de segurança?
a) Atualizações de programas que trazem novas funcionalidades.
b) Atualizações de programas que corrigem erros de software.
c) Atualizações de programas que melhoram a performance do computador.
d) Atualizações de programas que aumentam a capacidade de armazenamento.

08. O que é um software antivírus?
a) Um programa que permite baixar arquivos da internet.
b) Um programa que protege o computador contra vírus e outros tipos de *malware*.
c) Um programa que otimiza o desempenho do computador.
d) Todas as opções anteriores.

09. Por que é importante verificar os arquivos antes de fazer o download?
a) Para economizar tempo.
b) Para evitar baixar arquivos corrompidos.
c) Para proteger o computador contra vírus e *malware*.
d) Todas as opções anteriores.

10. O que é um arquivo malicioso?
a) Um arquivo que contém um vírus ou outro tipo de malware.
b) Um arquivo que não funciona corretamente.
c) Um arquivo que ocupa muito espaço no computador.
d) Um arquivo que é muito difícil de baixar.

11. Como um *software* antivírus pode proteger o computador contra arquivos maliciosos?
a) Analisando os arquivos antes de fazer o *download*.
b) Analisando os arquivos depois de fazer o *download*.
c) Desativando o *download* de arquivos desconhecidos.
d) Nenhuma das opções anteriores.

12. O que acontece se um arquivo malicioso é baixado no computador?
a) O computador pode ficar lento.
b) O arquivo malicioso pode infectar o computador com vírus ou *malware*.
c) O arquivo malicioso pode corromper outros arquivos no computador.
d) Todas as opções anteriores.

13. O que são redes Wi-Fi públicas ou gratuitas?
a) Redes Wi-Fi que são oferecidas gratuitamente por provedores seguros de internet.
b) Redes Wi-Fi que não possuem senha ou outra forma de autenticação para acessá-las.
c) Redes Wi-Fi que possuem uma camada extra de segurança.
d) Nenhuma das opções anteriores.

14. Por que as redes Wi-Fi públicas são perigosas?
a) Qualquer pessoa pode se conectar a elas.
b) Elas não possuem nenhum tipo de proteção ou autenticação.
c) Um cibercriminoso pode acessar tudo o que está armazenado no dispositivo conectado a ela.
d) Todas as opções anteriores.

15. O que pode acontecer se um dispositivo se conecta a uma rede Wi-Fi pública não segura?
a) O dispositivo pode ficar mais rápido.
b) O dispositivo pode receber atualizações de software automaticamente.
c) Um cibercriminoso pode acessar tudo o que está armazenado no dispositivo.
d) Nenhuma das opções anteriores.