

1. Malware são programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador. O programa de computador malicioso que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos é um tipo clássico de Malware denominado de

- A) backdoor.
- B) cavalo de troia.
- C) spyware.
- D) vírus.
- E) worm.

2. O correio eletrônico tornou-se uma ferramenta indispensável para atividades profissionais e pessoais, no entanto, muitos tipos de códigos maliciosos são introduzidos em computadores por meio dessa ferramenta. Assinale a opção que contém um tipo de código malicioso que NÃO pode ser recebido por e-mail.

- A) Worm.
- B) Rootkit.
- C) Trojan.
- D) Spyware.
- E) Vírus.

3. Assinale a alternativa que contém apenas códigos maliciosos capazes de alterar e remover arquivos do computador.

- A) Backdoor e Worm.
- B) Vírus e Trojan.
- C) Spyware e Worm.
- D) Bot e Rootkit.
- E) Vírus e Worm.

4. Sobre um SPAM é CORRETO afirmar que:

- A) É um vírus.
- B) É um antivírus.
- C) É uma mensagem de e-mail indesejada.
- D) É um navegador web.
- E) É um site de buscas.

5. O MS Windows XP dispõe de um utilitário para realizar backup. Com relação a esse utilitário seguem-se três afirmações:

- I - Permite realizar backup apenas para unidades de fita.
- II - Disponibiliza cinco tipos de backup: Normal, Cópia, Incremental, Diferencial e Diário.
- III - Possui a capacidade de fazer backup e restaurar o conteúdo de todo o computador ou de arquivos ou pastas específicas, incluindo arquivos em pastas compartilhadas em rede.

É correto apenas o que se afirma em:

- A) I
- B) II
- C) III
- D) I e II.
- E) II e III.

6. A Internet propicia muitas facilidades e tornou-se indispensável na atualidade. Ela expõe, porém, seus usuários a muitas ameaças. Uma das principais ameaças dos usuários da Internet são os vírus, que existem em diversas categorias. A categoria de vírus que visa a difundir histórias enganosas ou boatos é o

- A) Backdoor.
- B) Cavalo de Troia.
- C) Hoax.
- D) Phishing.
- E) Spyware.

7. Para trafegar informações pela Internet de forma segura, garantindo a integridade e sigilo, devemos fazer uso de:

- A) Criptografia.
- B) Firewall.
- C) Antivírus.
- D) Sniffer.
- E) Antispyware.

8. Qual o nome dado ao dispositivo de segurança que, uma vez instalado, controla e autoriza o tráfego de informações transferidas entre redes de computadores?

- A) Telnet
- B) Firewall.
- C) Cookie
- D) Safenet.
- E) Java

9. Das sentenças abaixo, relativas à segurança de computadores e sistemas,

- I. Um dos principais objetivos da criptografia é impedir a invasão de redes.
- II. O certificado digital é um arquivo eletrônico que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade.
- III. Um antivírus é capaz de impedir que um hacker tente explorar alguma vulnerabilidade existente em um computador.

IV. Vírus, keyloggers, worms e cavalos de tróia são alguns dos exemplos de Malware.

Estão corretas:

- A) I, II e III, apenas.
- B) I e IV, apenas.
- C) III e IV, apenas.
- D) I, II, III e IV.
- E) II e IV, apenas.

10. As redes de computadores e o advento da Internet trouxeram facilidades de comunicação através dos computadores, porém introduziram problemas de segurança de informações. Qual o nome do mecanismo em redes de computadores que controla e autoriza o tráfego de informações, estabelecendo filtros através de políticas de segurança?

- A) Cookie
- B) Proxy

- C) Telnet
- D) Winsock
- E) Firewall

11. O funcionário de uma empresa recebeu, pelo webmail, uma mensagem supostamente do banco no qual tem conta, informando que ele havia sido sorteado e ganhara um prêmio de um milhão de reais. Para resgatar o prêmio, o funcionário foi orientado a clicar em um link e digitar seus dados pessoais e bancários. Após seguir as orientações e enviar os dados digitados, percebeu que o endereço do banco era falso, mas muito semelhante ao endereço verdadeiro. O funcionário foi vítima de um tipo de fraude conhecida como

- A) Engenharia Social.
- B) worm.
- C) phishing.
- D) keylogging.
- E) Ransomware.

12. O tipo de código malicioso, que se instala em computadores, que torna inacessíveis os dados armazenados em um equipamento, muitas vezes usando criptografia, e que exige pagamento de resgate para restabelecer o acesso ao usuário é denominado

- A) Ransomware.
- B) RAT
- C) Backdoor.
- D) Worm.
- E) Bot.

13. Um problema de segurança ao navegar na internet pode tornar o computador indisponível e colocar em risco a confidencialidade e a integridade dos dados nele armazenados. Sobre navegação segura, associe a segunda coluna com a primeira.

- I) HTTP
- II) HTTPS
- III) EV SSL
- IV) Cookies

() Certificado que inclui a verificação de que a empresa foi legalmente registrada, encontra-se ativa e que detém o registro do domínio para o qual o certificado será emitido.

() Pequenos arquivos que são gravados no computador quando acessa sites na Internet e que são reenviados a estes mesmos sites quando novamente visitados.

() Protocolo que utiliza certificados digitais para assegurar a identidade, tanto do site de destino quanto da origem, caso possua.

() Protocolo sob o qual os dados trafegam sem criptografia.

Assinale a alternativa que contém a sequência CORRETA de associação, de cima para baixo.

- A) II, I, III, IV
- B) III, IV, II, I
- C) IV, II, III, I
- D) IV, III, II, I
- E) III, I, II, IV

14. Assinale a opção que contém a(s) afirmativa(s) **FALSA(S)** sobre senhas seguras.

- I - Devem conter informações pessoais.
- II - Devem conter diferentes tipos de caracteres.
- III - Devem conter grande quantidade de caracteres.
- A) Apenas I
- B) Apenas II
- C) Apenas I e III
- D) Apenas II e III
- E) I, II e III

15. Indique a opção que contém somente ferramentas importantes para a proteção de um computador.

- A) Firewall, bridge, antispayware
- B) Antivírus, bridge, protector
- C) Antivírus, firewall, antispayware
- D) Antivírus, bridge, firewall
- E) Antivírus, firewall, protector

16. Com relação aos conhecimentos sobre segurança na internet, julgue os itens abaixo:

I- O vírus é um programa ou parte de um programa de computador, para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o computador seja infectado é preciso que um programa já infectado seja executado.

II- O vírus de macro é um tipo específico de vírus de script, escrito em linguagem de macro, que tenta infectar arquivos que não seja manipulados por aplicativos.

III- Phishing é uma maneira desonesta que cibercriminosos usam para enganar o usuário e revelar suas informações.

IV- Spyware é um tipo de malware que hackers usam para espionar o usuário a fim de conseguir acesso às informações pessoais.

- A) Apenas o item I é falso.
- B) Os itens II e IV são verdadeiros.
- C) Apenas o item II é falso.
- D) Apenas os itens III e IV são verdadeiros
- E) Todos os itens são falsos.

17. Considere as duas situações em que a proteção e a segurança da informação foram violadas:

I. O número do CPF de um trabalhador foi alterado, deixando seu CPF inválido.

II. Um dado sigiloso de uma causa trabalhista foi acessado por uma pessoa não autorizada.

Nas situações I e II ocorreram, respectivamente, violação da

- A) autenticação e da autorização das informações.
- B) confidencialidade e da integridade das informações.
- C) confidencialidade e da disponibilidade das informações.
- D) identificação e da autorização das informações.
- E) integridade e da confidencialidade das informações.

1-D	2-B	3-B	4-C	5-E	6-C	7-A	8-B
9-E	10-E	11-C	12-A	13-B	14-A	15-C	16-C
17-E							