INFORMÁTICA

PROFESSOR: ANDRÉ ERICLES

SEGURANÇA

1)(CESPE/PRF 2019) No acesso a uma página web que contenha o código de um vírus de script, pode ocorrer a execução automática desse vírus, conforme as configurações do navegador. (C/E)

2)(CESPE/SEFAZ-RS 2019) Caso deseje evitar que cookies, histórico de sítios acessados e dados de formulários sejam gravados pelo programa navegador web enquanto acessa a Internet, o usuário deverá optar pelo uso de
A) teclado virtual. B) máquina virtual. C) antivírus.
D) bloqueador de pop-ups. E) navegação anônima.

4(CESPE/BNB 2018) Se um rootkit for removido de um sistema operacional, esse sistema não voltará à sua condição original, pois as mudanças nele implementadas pelo rootkit permanecerão ativas. (C/E)

5(CESPE/BNB 2018) Entre as categorias de antivírus disponíveis gratuitamente, a mais confiável e eficiente é o scareware, pois os antivírus dessa categoria fazem uma varredura nos arquivos e são capazes de remover 99% dos vírus existentes (C/E)

6(CEPSE/MPI-PI 2018) Foi solicitado a Paulo criptografar um pendrive, que contém arquivos sensíveis no sistema operacional Windows 10, de modo a proteger os dados desse dispositivo contra ameaças de roubo. Nessa situação, uma das formas de atender a essa solicitação é, por exemplo, utilizar a criptografia de unidade de disco BitLocker, um recurso de proteção de dados nesse sistema operacional. (C/E)

7(CEPSE/MPI-PI 2018) Ao acessar o sítio http://wwws.simp.mppi.mp.br/ para efetuar uma pesquisa sobre peças processuais, um usuário ficou em dúvida se deveria informar dados sigilosos. Nessa situação, a dúvida do usuário é improcedente, pois o fato de o sítio possuir um s (de secure) no endereço, especificamente em wwws., significa que todo acesso a esse sítio é seguro, uma vez que os dados trafegados entre o computador do usuário e o servidor são criptografados. (C/E)

8(CESPE/PF 2018) Formatos comuns de arquivos, como, por exemplo, .docx ou .xlsx, são utilizados como vetor de infecção por ransomware, um tipo de software malicioso que encripta os dados do usuário e solicita resgate. (C/E)

9(CESPE/PF 2018) A infecção de um sistema por códigos maliciosos pode ocorrer por meio da execução de arquivos infectados obtidos de anexos de mensagens eletrônicas, de mídias removíveis, de páginas web comprometidas, de redes sociais ou diretamente de outros equipamentos. (C/E)

10(CESPE/PF 2018) Um ataque de ransomware comumente ocorre por meio da exploração de vulnerabilidades de sistemas e protocolos; a forma mais eficaz de solucionar um ataque desse tipo e recuperar os dados “sequestrados” (criptografados) é a utilização de técnicas de quebra por força bruta da criptografia aplicada. (C/E)

11(CESPE/PF 2018) O sistema operacional utilizado na estação de trabalho de Marta inclui nativamente a plataforma Windows Defender, composta por ferramentas antivírus e de firewall pessoal, entre outras. (C/E)

12(CESPE/FUB 2016) Enquanto estiver conectado à Internet, um computador não será infectado por worms, pois este tipo de praga virtual não é transmitido pela rede de computadores. (C/E)

13(CESPE/INSS 2016) A infecção de um computador por vírus enviado via correio eletrônico pode se dar quando se abre arquivo infectado que porventura esteja anexado à mensagem eletrônica recebida. (C/E)

14(CESP/MEC 2014) A ação de worms pode afetar o desempenho de uma rede de computadores. (C/E)

15(CESPE/FUB 2015) Vírus é um programa autossuficiente capaz de se propagar automaticamente pelas redes enviando cópias de si mesmo de um computador para outro. (C/E)

16(CESPE/CM 2012) Os worms, assim como os vírus, infectam computadores, mas, diferentemente dos vírus, eles não precisam de um programa hospedeiro para se propagar. (C/E)

17(CESPE/TCE-RN 2015) A principal diferença entre crackers e hackers refere-se ao modo como esses malfeitores da área de segurança da informação atacam: os crackers são mais experientes e realizam ataques sem utilizar softwares, ao passo que os hackers utilizam códigos maliciosos associados aos softwares para realizar ataques ao ciberespaço. (C/E)

18(CESPE/ANS 2013) A contaminação por pragas virtuais ocorre exclusivamente quando o computador está conectado à Internet. (C/E)

19(CESPE/PC-DF 2013) Os vírus, ao se propagarem, inserem cópias de seu próprio código em outros programas, enquanto os worms se propagam pelas redes, explorando, geralmente, alguma vulnerabilidade de outros softwares. (C/E)

20(CESPE/FNDE 2012) Embora sejam considerados programas espiões, os spywares também são desenvolvidos por empresas com o objetivo de coletar legalmente informações acessíveis de usuários. (C/E)

21(CESPE/MDIC 2015) Um backdoor (porta dos fundos) é um programa de computador utilizado pelo administrador de rede para realizar a manutenção remota da máquina de um usuário. (C/E)

22(CESPE/TJ-AC 2012) Os rootkits são um conjunto de programas que oferecem mecanismos para esconder o invasor, assegurando a sua presença em um computador invadido. (C/E)

23(CESPE/CM 2012) Em cloud computing, cabe ao usuário do serviço se responsabilizar pelas tarefas de armazenamento, atualização e backup da aplicação disponibilizada na nuvem. (C/E)

24(CESPE/PF 2014) Computadores infectados por botnets podem ser controlados remotamente bem como podem atacar outros computadores sem que os usuários percebam. (C/E)

25) CESPE/PF 2014) Phishing é um tipo de malware que, por meio de uma mensagem de email, solicita informações confidenciais ao usuário, fazendo-se passar por uma entidade confiável conhecida do destinatário. (C/E)

26)(CESPE/TRT 17 2013) O fator de segurança da biometria é menor que o fator de segurança de outras soluções de identificação, como, por exemplo, o uso de cartões e de senhas. (C/E)

27(CESPE/CADE 2014) Os vírus de computador podem apagar arquivos criados pelo editor de texto, no entanto são incapazes de infectar partes do sistema operacional, já que os arquivos desse sistema são protegidos contra vírus. (C/E)