SUMÁRIO

QUESTÕES SOBRE A AULA

1 – **Ano:** 2013 **Banca:** CESPE **Órgão:** PC-BA **Prova:** Escrivão
A possibilidade de 'roubo de identidade' é problema de segurança comum relacionado ao uso de redes sociais, visto que dados para construção de perfis falsos de usuário são facilmente acessíveis a potenciais 'criminosos digitais'.
( ) Certo ( ) Errado

2 – **Ano:** 2018 **Banca:** aocp **Órgão:** UFOB **Prova:** Técnico em contabilidade
Ocorrências como: receber retorno de e-mails que não foram enviados por você; e verificar, nas notificações de acesso, que a sua conta de e-mail ou seu perfil na rede social foi acessado em horários ou locais em que você próprio não estava acessando são indicativos de que você está sendo fraudado com o golpe conhecido como Phishing.
( ) Certo ( ) Errado

3 – **Ano:** 2017 **Banca:** AOCP **Órgão:** UFBA **Prova:** Técnico em segurança do trabalho
Um exemplo de ataque por força bruta (brute force) seria adivinhar, por tentativa e erro, um nome de usuário e senha, por exemplo, e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios desse usuário.
( ) Certo ( ) Errado

4 – **Ano:** 2015 **Banca:** CESPE **Órgão:** Telebras **Prova:** Contador
Sniffers são programas aparentemente inofensivos cuja principal característica é utilizar a técnica de mascaramento. A técnica em questão permite, por exemplo, que um sniffer seja anexado a um jogo, que, por sua vez, ao ser instalado em um computador, coletará informações bancárias do usuário.
( ) Certo ( ) Errado

5 – **Ano:** 2015 **Banca:** CESPE **Órgão:** FUB **Prova:** Administrador
O phishing é um procedimento que possibilita a obtenção de dados sigilosos de usuários da Internet, em geral, por meio de falsas mensagens de email.
( ) Certo ( ) Errado

6 – **Ano:** 2015 **Banca:** CESPE **Órgão:** FUB **Prova:** Engenheiro Civil
Os Sniffers, utilizados para monitorar o tráfego da rede por meio da interceptação de dados por ela transmitidos, não podem ser utilizados por empresas porque violam as políticas de segurança da informação.
( ) Certo ( ) Errado

7 – **Ano:** 2013 **Banca:** CESPE **Órgão:** TJ – AC **Prova:** Analista Judiciário
Pharming é um ataque que possui como estratégia corromper o DNS e direcionar o endereço de um sítio para um servidor diferente do original.
( ) Certo ( ) Errado

8 – **Ano:** 2012 **Banca:** CESPE **Órgão:** Câmara dos Deputados **Prova:** Analista Legislativo
O termo spam refere-se a emails não solicitados e enviados, normalmente, apenas para uma pessoa; essa mensagem, cujo conteúdo é sempre comercial, não transporta vírus de computador ou links na Internet.
( ) Certo ( ) Errado

9 – **Ano:** 2012 **Banca:** CESPE **Órgão:** Câmara dos Deputados **Prova:** Analista Legislativo
O termo phishing designa a técnica utilizada por um fraudador para obter dados pessoais de usuários desavisados ou inexperientes, ao empregar informações que parecem ser verdadeiras com o objetivo de enganar esses usuários.
( ) Certo ( ) Errado

10 – **Ano:** 2012 **Banca:** CESPE **Órgão:** TRE – RJ **Prova:** Técnico Judiciário
Pharming é um tipo de golpe em que há o furto de identidade do usuário e o golpista tenta se passar por outra pessoa, assumindo uma falsa identidade roubada, com o objetivo de obter vantagens indevidas. Para evitar que isso aconteça, é recomendada a utilização de firewall , especificamente, o do tipo personal firewall.
( ) Certo ( ) Errado

11 – **Ano:** 2018 **Banca:** VUNESP **Órgão:** PC - SP **Prova:** Agente de comunicação Policial
Ao navegar pela Internet, deve-se tomar o cuidado para não ser vítima de um ataque conhecido como phishing. Uma das formas desse tipo de ataque é
A) a modificação do conteúdo de páginas web para apresentar propaganda ou dados falsos.
B) o roubo de dados pessoais como CPF e senha em comunicação que não utiliza o protocolo https.
C) a falsificação do certificado digital utilizado para acessar um site.
D) o roubo de dados pessoais e/ou financeiros utilizando páginas web falsas de comércio eletrônico.
E) o bloqueio do acesso a uma página web como se ela estivesse fora do ar.

12 – **Ano:** 2014 **Banca:** NUCEPE **Órgão:** PC - PI **Prova:** Escrivão
A utilização de práticas para obter acesso a informações sigilosas em organizações e sistemas computacionais, por meio da exploração de confiança das pessoas com habilidades de persuasão, é chamada de
A) engenharia reversa.
B) spyware.
C) engenharia social.
D) worm.
E) botnet.

13 – **Ano:** 2014 **Banca:** NUCEPE **Órgão:** PC - PI **Prova:** Escrivão
As mensagens de correio eletrônico enviadas não solicitadas, para fins publicitários, com caráter apelativo e na maioria das vezes inconvenientes são chamadas de
A) adware.
B) SPAM.
C) worm.
D) cavalo de tróia.
E) sniffer.

14 – **Ano:** 2013 **Banca:** FUMARC **Órgão:** PC - MG **Prova:** Analista
O tipo de ataque na Internet que tenta desativar os servidores de uma organização por meio de um grande conjunto de máquinas distribuídas que enviam dados ou fazem requisições simultâneas aos servidores da organização de forma excessiva é denominado.
A) DDoS
B) Phishing
C) Pharming
D) DNS Poisoning

15 – **Ano:** 2013 **Banca:** FUMARC **Órgão:** PC - MG **Prova:** Analista
Aplicações que capturam pacotes da rede e analisam suas características, também conhecidas como “farejadores" de pacotes, são
A) Banners
B) Worms
C) Spiders
D) Sniffers

16 - **Ano:** 2019 **Banca:** Instituto AOCP **Órgão:** Prefeitura de São Bento do Sul – SC **Prova:** Fiscal de Tributos
É uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um servidor, um computador ou uma rede conectada à Internet. O objetivo desses ataques não é invadir e nem coletar informações, mas sobrecarregar o alvo com a finalidade de torná-lo indisponível. A que o enunciado se refere?
A) Defacement.
B) Spoofing.
C) Sniffing.
D) DoS (Denial of Service).

17 – **Ano:** 2016 **Banca:** Instituto AOCP **Órgão:** CISAMUSEP - PR **Prova:** Teleatendente
É o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário. Ocorre geralmente por meio de mensagens eletrônicas falsas em nome de instituições conhecidas, geralmente tentando induzir o preenchimento de informações em páginas falsas. A que tipo de fraude o enunciado se refere?
A) Worm.
B) Bot e Botnet.
C) Backdoor.
D) Vírus.
E) Phishing.

18 – **Ano:** 2019 **Banca:** NC - UFPR **Órgão:** Prefeitura de Matinhos - PR **Prova:** Fiscal de tributos
Ao acessar o Internet Banking percebeu-se que o site não estava utilizando conexão segura. O suporte verificou que o serviço de DNS do computador estava redirecionando, de forma transparente, para uma página falsa. Esse tipo de ocorrência é chamada de:
A) sequestro de máquina.
B) ransomware.
C) pharming.
D) vírus.
E) fraude de antecipação de recursos.

19 – **Ano:** 2019 **Banca:** FCC **Órgão:** SPPREV **Prova:** Técnico em Gestão Previdenciária
Um dos procedimentos que mais potencializam as chances de ser vítima de um ataque de phishing é
A) acessar a conta de e-mail por meio de gerenciadores de e-mail como o Verse e o Notes SmartCloud.
B) excluir imediatamente e-mails com links de desconto ditos como imperdíveis durante uma campanha de comércio eletrônico.
C) acessar as contas de e-mail e redes sociais por meio de Wi-Fi público.

D) fornecer informações de login somente após verificar o nome do site e se ele inicia por "https".
E) abrir arquivos obsoletos, criados em versões de softwares que não possuem mais suporte do fabricante.

20 – **Ano:** 2017 **Banca:** FUNDEP **Órgão:** CISABRC-MG **Prova:** Assistente Administrativo
Assinale a alternativa que apresenta corretamente o termo usado para fazer referência aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas e que são associados a ataques à segurança da internet e do usuário.
A) Spam
B) Mala direta
C) Caixa de entrada
D) Antivírus

GABARITO

1 – Certo
2 – Errado
3 – Certo
4 – Errado
5 – Certo
6 – Errado
7 – Certo
8 – Errado
9 – Certo
10 – Errado
11 – D
12 – C
13 – B
14 – A
15 – D
16 – D
17 – E
18 – C
19 – C
20 - A

QUESTÕES COMENTADAS

1 – **Ano:** 2013 **Banca:** CESPE **Órgão:** PC-BA **Prova:** Escrivão
A possibilidade de 'roubo de identidade' é problema de segurança comum relacionado ao uso de redes sociais, visto que dados para construção de perfis falsos de usuário são facilmente acessíveis a potenciais 'criminosos digitais'.
( ) Certo ( ) Errado

Gabarito: Certo

O Furto de identidade é o ato de uma pessoa tentar se passar por outra utilizando uma identidade falsa. A forma mais comum de furto de identidade é através da criação de um perfil falso como um perfil em rede social. Quanto mais informações públicas você disponibilizar na redes sócias mais vulnerável você estará de ser vítima desse tipo de golpe.

O furto de identidade, ou identity theft, é o ato pelo qual uma pessoa tenta se passar por outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens indevidas. Alguns casos de furto de identidade podem ser considerados como crime contra a fé pública, tipificados como falsa identidade.

No seu dia a dia, sua identidade pode ser furtada caso, por exemplo, alguém abra uma empresa ou uma conta bancária usando seu nome e seus documentos. Na Internet isto também pode ocorrer, caso alguém crie um perfil em seu nome em uma rede social, acesse sua conta de e-mail e envie mensagens se passando por você ou falsifique os campos de e-mail, fazendo parecer que ele foi enviado por você.

Quanto mais informações você disponibiliza sobre a sua vida e rotina, mais fácil se torna para um golpista furtar a sua identidade, pois mais dados ele tem disponíveis e mais convincente ele pode ser. Além disto, o golpista pode usar outros tipos de golpes e ataques para coletar informações sobre você, inclusive suas senhas, como códigos, ataques de força bruta e interceptação de tráfego.

2 – **Ano:** 2018 **Banca:** aocp **Órgão:** UFOB **Prova:** Técnico em contabilidade
Ocorrências como: receber retorno de e-mails que não foram enviados por você; e verificar, nas notificações de acesso, que a sua conta de e-mail ou seu perfil na rede social foi acessado em horários ou locais em que você próprio não estava acessando são indicativos de que você está sendo fraudado com o golpe conhecido como Phishing.
( ) Certo ( ) Errado

Gabarito: Errada

Phishing, phishing-scam ou phishing/scam, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social. Receber notificações com respostas de mensagens que você não enviou é um indicio de que você foi vítima de Roubo de Identidade.

O furto de identidade, ou identity theft, é o ato pelo qual uma pessoa tenta se passar por outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens indevidas. Alguns casos de furto de identidade podem ser considerados como crime contra a fé pública, tipificados como falsa identidade.

A melhor forma de impedir que sua identidade seja furtada é evitar que o impostor tenha acesso aos seus dados e às suas contas de usuário (mais detalhes no Capítulo Privacidade). Além disto, para evitar que suas senhas sejam obtidas e indevidamente usadas, é muito importante que você seja cuidadoso, tanto ao usá-las quanto ao elaborá-las

É necessário também que você fique atento a alguns indícios que podem demonstrar que sua identidade está sendo indevidamente usada por golpistas, tais como:

- você começa a ter problemas com órgãos de proteção de crédito;
- você recebe o retorno de e-mails que não foram enviados por você;
- você verifica nas notificações de acesso que a sua conta de e-mail ou seu perfil na rede social foi acessado em horários ou locais em que você próprio não estava acessando;

ao analisar o extrato da sua conta bancária ou do seu cartão de crédito você percebe transações que não foram realizadas por você;

- você recebe ligações telefônicas, correspondências e e-mails se referindo a assuntos sobre os quais você não sabe nada a respeito, como uma conta bancária que não lhe pertence e uma compra não realizada por você.

3 – **Ano:** 2017 **Banca:** AOCP **Órgão:** UFBA **Prova:** Técnico em segurança do trabalho

Um exemplo de ataque por força bruta (brute force) seria adivinhar, por tentativa e erro, um nome de usuário e senha, por exemplo, e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios desse usuário.

( ) Certo ( ) Errado

Gabarito: Certo

O ataque de força bruta consiste em um ataque de tentativa e erro, muitas vezes usado para quebra de senhas de usuários a partir de informações básicas que usuários tipicamente utilizam como senha.

Um ataque de força bruta, ou brute force, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário.

Qualquer computador, equipamento de rede ou serviço que seja acessível via Internet, com um nome de usuário e uma senha, pode ser alvo de um ataque de força bruta. Dispositivos móveis, que estejam protegidos por senha, além de poderem ser atacados pela rede, também podem ser alvo deste tipo de ataque caso o atacante tenha acesso físico a eles.

Se um atacante tiver conhecimento do seu nome de usuário e da sua senha ele pode efetuar ações maliciosas em seu nome como, por exemplo:

- trocar a sua senha, dificultando que você acesse novamente o site ou computador invadido;

- invadir o serviço de e-mail que você utiliza e ter acesso ao conteúdo das suas mensagens e à sua lista de contatos, além de poder enviar mensagens em seu nome;

- acessar a sua rede social e enviar mensagens aos seus seguidores contendo códigos maliciosos ou alterar as suas opções de privacidade;

- invadir o seu computador e, de acordo com as permissões do seu usuário, executar ações, como apagar arquivos, obter informações confidenciais e instalar códigos maliciosos.

Mesmo que o atacante não consiga descobrir a sua senha, você pode ter problemas ao acessar a sua conta caso ela tenha sofrido um ataque de força bruta, pois muitos sistemas bloqueiam as contas quando várias tentativas de acesso sem sucesso são realizadas.

Apesar dos ataques de força bruta poderem ser realizados manualmente, na grande maioria dos casos, eles são realizados com o uso de ferramentas automatizadas facilmente obtidas na Internet e que permitem tornar o ataque bem mais efetivo.

As tentativas de adivinhação costumam ser baseadas em:

- dicionários de diferentes idiomas e que podem ser facilmente obtidos na Internet;

- listas de palavras comumente usadas, como personagens de filmes e nomes de times de futebol;

- substituições óbvias de caracteres, como trocar "a" por "@" e "o" por "0"';

- sequências numéricas e de teclado, como "123456", "qwert" e "1qaz2wsx";

- informações pessoais, de conhecimento prévio do atacante ou coletadas na Internet em redes sociais e blogs, como nome, sobrenome, datas e números de documentos.

Um ataque de força bruta, dependendo de como é realizado, pode resultar em um ataque de negação de serviço, devido à sobrecarga produzida pela grande quantidade de tentativas realizadas em um pequeno período de tempo (mais detalhes no Capítulo Contas e senhas).

4 – **Ano:** 2015 **Banca:** CESPE **Órgão:** Telebras **Prova:** Contador

Sniffers são programas aparentemente inofensivos cuja principal característica é utilizar a técnica de mascaramento. A técnica em questão permite, por exemplo, que um sniffer seja anexado a um jogo, que, por sua vez, ao ser instalado em um computador, coletará informações bancárias do usuário.

( ) Certo ( ) Errado

Gabarito: Errado

O Sniffer é um programa malicioso que analisa tráfego de dados em busca de dados em busca de dados do usuário como senhas e dados bancários.

O termo sniffing pode ser aplicado tanto ao ataque como ao ato em si, como ao usuário ou programa usado para realizar o processo. Sniffing consiste em escutar

a rede. Esse procedimento não indica necessariamente em ato indevido, pois é uma prática necessária também para avaliar a comunicação de uma rede e também a proteger, como no caso dos IDSs.

5 – **Ano:** 2015 **Banca:** CESPE **Órgão:** FUB **Prova:** Administrador

O phishing é um procedimento que possibilita a obtenção de dados sigilosos de usuários da Internet, em geral, por meio de falsas mensagens de email.

( ) Certo ( ) Errado

Gabarito: Certa

Phishing, phishing-scam ou phishing/scam, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

Phishing, phishing-scam ou phishing/scam, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

O phishing ocorre por meio do envio de mensagens eletrônicas que:

- tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um site popular;

- procuram atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;

- informam que a não execução dos procedimentos descritos pode acarretar sérias consequências, como a inscrição em serviços de proteção de crédito e o cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito;

- tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição; da instalação de códigos maliciosos, projetados para coletar informações sensíveis; e do preenchimento de formulários contidos na mensagem ou em páginas Web.

Para atrair a atenção do usuário as mensagens apresentam diferentes tópicos e temas, normalmente explorando campanhas de publicidade, serviços, a imagem de pessoas e assuntos em destaque no momento. Exemplos de situações envolvendo phishing são:

- Páginas falsas de comércio eletrônico ou Internet Banking: você recebe um e-mail, em nome de um site de comércio eletrônico ou de uma instituição financeira, que tenta induzi-lo a clicar em um link. Ao fazer isto, você é direcionado para uma página Web falsa, semelhante ao site que você realmente deseja acessar, onde são solicitados os seus dados pessoais e financeiros.

- Páginas falsas de redes sociais ou de companhias aéreas: você recebe uma mensagem contendo um link para o site da rede social ou da companhia aérea que você utiliza. Ao clicar, você é direcionado para uma página Web falsa onde é solicitado o seu nome de usuário e a sua senha que, ao serem fornecidos, serão enviados aos golpistas que passarão a ter acesso ao site e poderão efetuar ações em seu nome, como enviar mensagens ou emitir passagens aéreas.

- Mensagens contendo formulários: você recebe uma mensagem eletrônica contendo um formulário com campos para a digitação de dados pessoais e financeiros. A mensagem solicita que você preencha o formulário e apresenta um botão para confirmar o envio das informações. Ao preencher os campos e confirmar o envio, seus dados são transmitidos para os golpistas.

- Mensagens contendo links para códigos maliciosos: você recebe um e-mail que tenta induzi-lo a clicar em um link, para baixar e abrir/executar um arquivo. Ao clicar, é apresentada uma mensagem de erro ou uma janela pedindo que você salve o arquivo. Após salvo, quando você abri-lo/executá-lo, será instalado um código malicioso em seu computador.

- Solicitação de recadastramento: você recebe uma mensagem, supostamente enviada pelo grupo de suporte da instituição de ensino que frequenta ou da empresa em que trabalha, informando que o serviço de e-mail está passando por manutenção e que é necessário o recadastramento. Para isto, é preciso que você forneça seus dados pessoais, como nome de usuário e senha.

6 – **Ano:** 2015 **Banca:** CESPE **Órgão:** FUB **Prova:** Engenheiro Civil

Os Sniffers, utilizados para monitorar o tráfego da rede por meio da interceptação de dados por ela transmitidos, não podem ser utilizados por empresas porque violam as políticas de segurança da informação.

( ) Certo ( ) Errado

Gabarito: Errado

Sniffing consiste em escutar a rede. Esse procedimento não indica necessariamente em ato indevido, pois é uma prática necessária também para avaliar a comunicação de uma rede e também a proteger, como no caso dos IDSs.

7 – **Ano:** 2013 **Banca:** CESPE **Órgão:** TJ – AC **Prova:** Analista Judiciário

Pharming é um ataque que possui como estratégia corromper o DNS e direcionar o endereço de um sítio para um servidor diferente do original.

( ) Certo ( ) Errado

Gabarito: Certa

Pharming é um tipo específico de phishing que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS (Domain Name System). Neste caso, quando você tenta acessar um site legítimo, o seu navegador Web é redirecionado, de forma transparente, para uma página falsa.

Também conhecido como DNS cache Poison ou DNS cache poisoning (envenenamento de cache DNS), pode ainda ser mencionado como Sequestro de DNS. Essa técnica de ataque consiste em redirecionar o usuário que busca acessar a um site legítimo a outro endereço com conteúdo adverso, normalmente um site falso (phishing).

Essa manipulação pode ocorrer de dois modos:

- Localmente: quando um malware altera o cache de DNS do navegador;

- Em escala: quando o cracker (hacker black hat) consegue fraldar a estrutura de cache de DNS que o usuário acessa em busca do endereço IP do site legítimo;

8 – **Ano:** 2012 **Banca:** CESPE **Órgão:** Câmara dos Deputados **Prova:** Analista Legislativo

O termo spam refere-se a emails não solicitados e enviados, normalmente, apenas para uma pessoa; essa mensagem, cujo conteúdo é sempre comercial, não transporta vírus de computador ou links na Internet.

( ) Certo ( ) Errado

Gabarito: Errada

Spam do ponto de vista da pessoa que envia a mensagem é a propagação em massa de mensagens. Já do ponto de vista de que recebe a mensagem, spam é uma mensagem indesejada. A disseminação dos Spam serve para aplicar golpes, espalhar programas maliciosos e Hoax (boatos).

Spam é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando este tipo de mensagem possui conteúdo exclusivamente comercial também é referenciado como UCE (Unsolicited Commercial E-mail).

O spam em alguns pontos se assemelha a outras formas de propaganda, como a carta colocada na caixa de correio, o panfleto recebido na esquina e a ligação telefônica ofertando produtos. Porém, o que o difere é justamente o que o torna tão atraente e motivante para quem o envia (spammer): ao passo que nas demais formas o remetente precisa fazer algum tipo de investimento, o spammer necessita investir muito pouco, ou até mesmo nada, para alcançar os mesmos objetivos e em uma escala muito maior.

Desde o primeiro spam registrado e batizado como tal, em 1994, essa prática tem evoluído, acompanhando o desenvolvimento da Internet e de novas aplicações e tecnologias. Atualmente, o envio de spam é uma prática que causa preocupação, tanto pelo aumento desenfreado do volume de mensagens na rede, como pela natureza e pelos objetivos destas mensagens.

9 – **Ano:** 2012 **Banca:** CESPE **Órgão:** Câmara dos Deputados **Prova:** Analista Legislativo

O termo phishing designa a técnica utilizada por um fraudador para obter dados pessoais de usuários desavisados ou inexperientes, ao empregar informações que parecem ser verdadeiras com o objetivo de enganar esses usuários.
( ) Certo ( ) Errado

Gabarito: Certo

Phishing ocorre quando um usuário tenta se passar por pessoa confiável para obter dados sigilosos ou algum outro tipo de vantagem. Basicamente, esse golpe engana o usuário fazendo uma informação ou documento falso se passar por verdadeira. Phishing també pode ser chamado de Golpe de Engenharia Social.

Phishing, phishing-scam ou phishing/scam, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

Para atrair a atenção do usuário as mensagens apresentam diferentes tópicos e temas, normalmente explorando campanhas de publicidade, serviços, a imagem de pessoas e assuntos em destaque no momento.

10 – **Ano:** 2012 **Banca:** CESPE **Órgão:** TRE – RJ **Prova:** Técnico Judiciário
Pharming é um tipo de golpe em que há o furto de identidade do usuário e o golpista tenta se passar por outra pessoa, assumindo uma falsa identidade roubada, com o objetivo de obter vantagens indevidas. Para evitar que isso aconteça, é recomendada a utilização de firewall , especificamente, o do tipo personal firewall.
( ) Certo ( ) Errado

Gabarito: Errada

Pharming é uma técnica de ataque consiste adulterar a tabela do DNS e redirecionar o usuário que busca acessar a um site legítimo para outro endereço com conteúdo adverso, normalmente um site falso (phishing).

O Firewall é uma ferramenta de segurança que visa proteger a rede local de ataques advindos da internet. O firewall não faz a validação do endereço acessado pelo usuário no DNS, consequentemente o Firewall não protege o usuário contra golpes de Pharming.

11 – **Ano:** 2018 **Banca:** VUNESP **Órgão:** PC - SP **Prova:** Agente de comunicação Policial
Ao navegar pela Internet, deve-se tomar o cuidado para não ser vítima de um ataque conhecido como phishing. Uma das formas desse tipo de ataque é
A) a modificação do conteúdo de páginas web para apresentar propaganda ou dados falsos.
B) o roubo de dados pessoais como CPF e senha em comunicação que não utiliza o protocolo https.
C) a falsificação do certificado digital utilizado para acessar um site.
D) o roubo de dados pessoais e/ou financeiros utilizando páginas web falsas de comércio eletrônico.
E) o bloqueio do acesso a uma página web como se ela estivesse fora do ar.

Gabarito: Letra D

Phishing, phishing-scam ou phishing/scam, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

Para atrair a atenção do usuário as mensagens apresentam diferentes tópicos e temas, normalmente explorando campanhas de publicidade, serviços, a imagem de pessoas e assuntos em destaque no momento.

O phishing ocorre por meio do envio de mensagens eletrônicas que:

- Tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um site popular;
- Procuram atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;
- Informam que a não execução dos procedimentos descritos pode acarretar sérias consequências, como a inscrição em serviços de proteção de crédito e o cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito;
- Tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição; da instalação de códigos maliciosos, projetados para coletar informações sensíveis; e do preenchimento de formulários contidos na mensagem ou em páginas Web.

12 – **Ano:** 2014 **Banca:** NUCEPE **Órgão:** PC - PI **Prova:** Escrivão

A utilização de práticas para obter acesso a informações sigilosas em organizações e sistemas computacionais, por meio da exploração de confiança das pessoas com habilidades de persuasão, é chamada de

A) engenharia reversa.
B) spyware.
C) engenharia social.
D) worm.
E) botnet.

Gabarito: Letra C

Engenharia Social é a habilidade de conseguir acesso a informações confidenciais ou a áreas importantes de uma instituição através de habilidades de persuasão. Na prática a Engenharia social é enganar alguém para obter informações sigilosas, é comum em prova fazer referência ao termo engenharia social como sinônimo de Phishing.

13 – **Ano:** 2014 **Banca:** NUCEPE **Órgão:** PC - PI **Prova:** Escrivão

As mensagens de correio eletrônico enviadas não solicitadas, para fins publicitários, com caráter apelativo e na maioria das vezes inconvenientes são chamadas de

A) adware.
B) SPAM.
C) worm.
D) cavalo de tróia.
E) sniffer.

Gabarito: Letra B

Spam é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

Letra A: Adware é um tipo de Spyware que inclui propagandas na máquina do usuário.

Letra B: SPAM é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

Letra C: Worm é o programa malicioso que cria cópias de si mesmo e se espalha de computador em computador.

Letra D: Cavalo de Tróia é o malware que aparentemente é inofensivo, porém cria vulnerabilidades. Um software que além da finalidade para o qual foi criado, executa ações maliciosas.

Letra E: Sniffer é um programa malicioso que analisa tráfego de dados em busca de dados em busca de dados do usuário como senhas e dados bancários.

14 – **Ano:** 2013 **Banca:** FUMARC **Órgão:** PC - MG **Prova:** Analista

O tipo de ataque na Internet que tenta desativar os servidores de uma organização por meio de um grande conjunto de máquinas distribuídas que enviam dados ou fazem requisições simultâneas aos servidores da organização de forma excessiva é denominado.

A) DDoS
B) Phishing
C) Pharming
D) DNS Poisoning

Gabarito: Letra A

DDoS (distributed denial of servisse) é um ataque de negação de serviço, ou seja, é um ataque que visa indisponilizar (derrubar) um serviço, deixando-o fora do ar. O tipo de DDoS mais comum é o Botnet que utiliza milhares de máquinas zumbis para atacar sistemas.

15 – **Ano:** 2013 **Banca:** FUMARC **Órgão:** PC - MG **Prova:** Analista

Aplicações que capturam pacotes da rede e analisam suas características, também conhecidas como “farejadores" de pacotes, são

A) Banners
B) Worms
C) Spiders
D) Sniffers

Gabarito: Letra D

Sniffer consiste em escutar a rede, analisando os pacotes de dados. Pode ser usado para interceptar dados do usuário como senhas e dados bancários . Esse procedimento não indica necessariamente em ato indevido, pois é uma prática

necessária também para avaliar a comunicação de uma rede e também a proteger, como no caso dos IDSs.

16 - **Ano:** 2019 **Banca:** Instituto AOCP **Órgão:** Prefeitura de São Bento do Sul – SC **Prova:** Fiscal de Tributos

É uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um servidor, um computador ou uma rede conectada à Internet. O objetivo desses ataques não é invadir e nem coletar informações, mas sobrecarregar o alvo com a finalidade de torná-lo indisponível. A que o enunciado se refere?

A) Defacement.
B) Spoofing.
C) Sniffing.
D) DoS (Denial of Service).

Gabarito: Letra D

Negação de serviço, ou DoS (Denial of Service), é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

Letra A: Defacement é a desfiguração de página, defacement ou pichação, é uma técnica que consiste em alterar o conteúdo da página Web de um site.

Letra B: Spoofing pode ser definido como disfarçar algo, usar algo falso. Ip Spoofing é usar um IP Falso. Mail Spoofin é um e-mail falso.

Letra C: Sniffing é também chamado de interceptação de tráfego, é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de sniffers.

Letra D: DoS é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

17 – **Ano:** 2016 **Banca:** Instituto AOCP **Órgão:** CISAMUSEP - PR **Prova:** Teleatendente

É o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário. Ocorre geralmente por meio de mensagens eletrônicas falsas em nome de instituições conhecidas, geralmente tentando induzir o preenchimento de informações em páginas falsas. A que tipo de fraude o enunciado se refere?

A) Worm.
B) Bot e Botnet.
C) Backdoor.
D) Vírus.
E) Phishing.

Gabarito: Letra E.

Phishing, phishing-scam ou phishing/scam, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

Para atrair a atenção do usuário as mensagens apresentam diferentes tópicos e temas, normalmente explorando campanhas de publicidade, serviços, a imagem de pessoas e assuntos em destaque no momento.

18 – **Ano:** 2019 **Banca:** NC - UFPR **Órgão:** Prefeitura de Matinhos - PR **Prova:** Fiscal de tributos
Ao acessar o Internet Banking percebeu-se que o site não estava utilizando conexão segura. O suporte verificou que o serviço de DNS do computador estava redirecionando, de forma transparente, para uma página falsa. Esse tipo de ocorrência é chamada de:
A) sequestro de máquina.
B) ransomware.
C) pharming.
D) vírus.
E) fraude de antecipação de recursos.

Gabarito: Letra C
Pharming é um tipo específico de phishing que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS (Domain Name System). Neste caso, quando você tenta acessar um site legítimo, o seu navegador Web é redirecionado, de forma transparente, para uma página falsa.

19 – **Ano:** 2019 **Banca:** FCC **Órgão:** SPPREV **Prova:** Técnico em Gestão Previdenciária
Um dos procedimentos que mais potencializam as chances de ser vítima de um ataque de phishing é
A) acessar a conta de e-mail por meio de gerenciadores de e-mail como o Verse e o Notes SmartCloud.
B) excluir imediatamente e-mails com links de desconto ditos como imperdíveis durante uma campanha de comércio eletrônico.
C) acessar as contas de e-mail e redes sociais por meio de Wi-Fi público.
D) fornecer informações de login somente após verificar o nome do site e se ele inicia por "https".
E) abrir arquivos obsoletos, criados em versões de softwares que não possuem mais suporte do fabricante.

Gabarito: Letra C
Ao utilizar um rede Wi-Fi pública você também corre risco de ser vítima de Pharming pois pode haver a configuração de redirecionamento para a página falsa dentro da própria rede. Você pode digitar, por exemplo, o endereço do Internet Banking e o Roteador da rede, já previamente configurado para isso, pode direcionar suas requisições para o site falso.

20 – **Ano:** 2017 **Banca:** FUNDEP **Órgão:** CISABRC-MG **Prova:** Assistente Administrativo
Assinale a alternativa que apresenta corretamente o termo usado para fazer referência aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas e que são associados a ataques à segurança da internet e do usuário.
A) Spam
B) Mala direta

C) Caixa de entrada
D) Antivírus

Gabarito: Letra A

Spam é o envio massivo de mensagens que para o usuário que recebe é considerado como mensagens indesejadas. Pode ser usado para Propagar Malwares, Hoax e Phishing.

Spam é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

O spam em alguns pontos se assemelha a outras formas de propaganda, como a carta colocada na caixa de correio, o panfleto recebido na esquina e a ligação telefônica ofertando produtos. Porém, o que o difere é justamente o que o torna tão atraente e motivante para quem o envia (spammer): ao passo que nas demais formas o remetente precisa fazer algum tipo de investimento, o spammer necessita investir muito pouco, ou até mesmo nada, para alcançar os mesmos objetivos e em uma escala muito maior.