CURSO ON-LINE – NOÇÕES DE INFORMÁTICA (TEORIA E EXERCÍCIOS) P/SENADO FEDERAL
PROFESSORES: PATRÍCIA QUINTÃO E ALEXANDRE LÊNIN

AULA 0 – APRESENTAÇÃO

Olá pessoal, nossos cumprimentos!!!

Estamos aqui no Ponto para mais um curso on-line da disciplina **Noções de Informática (Teoria e Exercícios)**, visando o concurso do **Senado Federal** com foco na banca **FGV**.

Este curso está organizado de acordo com o edital do último concurso para o Senado Federal. Se o edital for lançado no decorrer deste curso, as aulas ainda não lecionadas serão adaptadas visando adequar ao máximo ao novo edital. Procuraremos utilizar exercícios da banca oficial, os assuntos desnecessários serão retirados da programação do curso e, no lugar dos tópicos descartados serão incluídos assuntos que porventura não estejam contemplados neste curso – considerando a quantidade de aulas restantes.

A satisfação e motivação estão cada vez maiores, e será um enorme prazer trabalhar com cada um de vocês neste curso rumo ao tão sonhado cargo público!

Para nós, é muito importante fazer parte desta conquista. Nossa tarefa é transmitir o conteúdo na forma de resolução de exercícios com didática e objetividade, de forma a facilitar o aprendizado. Cumpriremos o objetivo com muita seriedade e dedicação.

Bem, antes de falarmos sobre o curso, façamos uma breve apresentação. Vamos lá!

CURSO ON-LINE – NOÇÕES DE INFORMÁTICA (TEORIA E EXERCÍCIOS) P/SENADO FEDERAL
PROFESSORES: PATRÍCIA QUINTÃO E ALEXANDRE LÊNIN

A professora Patrícia Lima Quintão, 37 anos, leciona em cursos preparatórios para concursos desde 2003, já tendo dado aulas de informática em cursos presenciais e em inúmeros cursos *on-line* do Ponto dos Concursos (visando certames como Polícia Federal, MPU, TCU, Ministério da Fazenda, MPOG, PRF, SEFAZ/RJ, dentre outros). Também leciona disciplinas técnicas do curso de Sistemas de Informação e Ciência da Computação, tanto na graduação, quanto na pós-graduação, além de coordenar a área de Segurança da Informação na Prefeitura de Juiz de Fora (MG). Uma novidade é que no próximo mês também já estará lançando o seu primeiro livro de "Questões Comentadas de Informática com foco na banca FCC"!! Espero que aproveitem!!

Quanto à sua formação, é mestre em Engenharia de Sistemas e Computação pela COPPE/UFRJ, pós-graduada em Gerência de Informática e bacharel em Informática pela UFV. Também atua como membro da Sociedade Brasileira de Computação e do Comitê Brasileiro de Processamento de Dados da ABNT, que cria as normas sobre gestão da Segurança da Informação no Brasil; tem certificações técnicas na área de segurança, redes e perícia forense; além de artigos publicados a nível nacional e internacional com temas da nossa área.

E como não poderia deixar de ser, nas horas vagas, também é concurseira, já tendo sido nomeada para assumir o cargo em vários concursos, como Analista de Sistemas no SERPRO (2001 e 2005); Analista Judiciário (Área de Informática) no Tribunal Regional Federal - 2ª Região (2003); Professora titular do Departamento de Ciência da Computação do Instituto Federal de Educação, Ciência e Tecnologia (2010), dentre outros.

CURSO ON-LINE – NOÇÕES DE INFORMÁTICA (TEORIA E EXERCÍCIOS) P/SENADO FEDERAL
PROFESSORES: PATRÍCIA QUINTÃO E ALEXANDRE LÊNIN

O professor Alexandre Lênin Carneiro, 38 anos, é Analista de Planejamento e Orçamento do Ministério do Planejamento, da área de Tecnologia da Informação. Trabalha na Coordenação de Sistemas de Planejamento, acompanhando o desenvolvimento e manutenção dos principais sistemas da Secretaria, participando dos grupos de trabalho da área de Tecnologia da Informação e dos processos de contratação de serviços de Tecnologia da Informação para o Ministério, além de participar da gestão técnica do Portal do Planejamento.

É professor de informática desde os 18 anos (1990), tendo lecionado em cursos técnicos, graduação e pós-graduação. Também é Mestre em Ciência da Computação pela UnB, com formação na área de Inteligência Artificial. No serviço público, foi funcionário do Serpro, Ibama e Receita Federal.

Bem, passada a apresentação inicial, esperamos que este curso seja de grande valia para o seu estudo, fazendo-o superar os desafios vindouros na prova!

Organização do curso

O curso será iniciado em **27/09/2010**, indo até **15/11/2010**, com o cronograma/conteúdo listado no quadro a seguir.

AULA	DATA	CONTEÚDO DAS AULAS
0		**Aula Inaugural** – Proposta do curso e questões de Demonstração sobre o tema "Noções de Segurança e Proteção".
1	27/09	**Microsoft Word** em português: edição e formatação de textos (operações do menu Formatar, Inserir,

		Tabelas, Exibir - cabeçalho e rodapé, Arquivo – configurar página e impressão, Ferramentas – ortografia e gramática).
2	04/10	**Microsoft Excel** em português: criação de pastas, planilhas e gráficos, uso de formulas, funções e macros, configurar página, impressão, operações do menu Formatar, operações do menu Inserir, obtenção de dados externos, classificar.
3	11/10	**Microsoft Windows XP** em português: Criação de pastas (diretórios), arquivos e atalhos, área de trabalho, área de transferência, manipulação de arquivos e pastas, uso dos menus, uso de aplicativos, interação com os aplicativos do Microsoft Office.
4	18/10	**Redes Microsoft**: conceitos básicos de redes, compartilhamento de pastas e arquivos; localização e utilização de computadores e pastas remotas. **Noções de Segurança da Informação.**
5	25/10	**Internet e Tópicos Relacionados**: conceitos básicos, navegação Internet, conceitos de URL, links, sites, impressão de páginas.
6	01/11	**Correio Eletrônico** (mensagens, anexação de arquivos, cópias).
7	08/11	**BrOffice Writer**: editor de textos do pacote BrOffice.org
8	15/11	**BrOffice Excel**: planilha eletrônica do pacote BrOffice.org

ATENÇÃO: esta é uma aula demonstrativa para que você possa avaliar o nosso trabalho. Para esta demonstração, selecionamos o tema conceitos básicos de segurança da informação.

As demais aulas estão estruturadas conforme a tabela anterior, dando ênfase aos conteúdos de maior relevância a este certame, considerando sempre o edital do último concurso. Nas demais **oito aulas** de Informática serão apresentadas mais de 160 questões (em média teremos cerca de 20 questões por aula) a fim de familiarizar você com o estilo de questões normalmente utilizado pela banca.

Cabe destacar que, de forma complementar, em alguns momentos serão criadas novas questões ou apresentadas questões de outras bancas (como CESGRANRIO, FCC e CESPE) para complementar ou mesmo para introduzir um determinado conteúdo. Sempre que fizermos isso será levando em conta o formato e a profundidade das questões de informática que costumamos encontrar nas provas da FGV.

Por fim, para aqueles que venham a se matricular no curso, ainda teremos o fórum para troca de informações e/ou esclarecimento de dúvidas que porventura surgirem. Críticas e/ou sugestões são bem-vindas!

Grande abraço,

Patrícia e Lênin

Sem mais delongas, comecemos a aula demonstrativa sobre segurança da informação.

Aula 0 – Demonstrativa

Noções de segurança e proteção.

O que significa SEGURANÇA?

É colocar tranca nas portas de sua casa? É ter as suas informações guardadas de forma suficientemente segura para que pessoas sem autorização não tenham acesso a elas? Vamos nos preparar para que a próxima vítima não seja você ☺!!!

A **segurança** é uma palavra que está presente em nosso cotidiano e refere-se a um estado de proteção, em que estamos "livres" de perigos e incertezas.

A Tecnologia da informação só se torna uma ferramenta capaz de alavancar verdadeiramente os negócios, quando seu uso está vinculado às medidas de proteção dos dados corporativos, para assegurar a sobrevivência da empresa e a continuidade dos negócios da organização.

Segurança da informação é o processo de proteger a informação de diversos tipos de ameaças externas e internas para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio.

Soluções pontuais isoladas não resolvem toda a problemática associada à segurança da informação. Segurança se faz em pedaços, porém todos eles integrados, como se fossem uma corrente.

Isso reafirma o ditado popular, muito citado pelos especialistas em segurança, que diz que nenhuma corrente é mais forte do que o seu elo mais fraco. De nada adianta uma corrente ser a mais resistente de todas se existe um elo que é fraco. É claro que a resistência da corrente será a resistência do elo mais fraco e não dos demais. Se a corrente passar por um teste de esforço, certamente o elo que partirá será o mais fraco.

Essa mesma ideia aplica-se ao contexto da informação. Quando precisamos garantir a segurança da informação, precisamos eliminar os "elos fracos" do ambiente em que a informação está armazenada. Já que eliminar, neste contexto é sempre difícil, então buscamos sempre reduzir ao máximo os riscos de que a segurança da informação seja violada.

A segurança da informação não deve ser tratada como um fator isolado e tecnológico apenas, mas sim como a **gestão inteligente da informação em todos os ambientes, desde o ambiente tecnológico passando pelas aplicações, infraestrutura e as pessoas**.

Segurança se faz protegendo todos os elos da corrente, ou seja, todos os ativos (físicos, tecnológicos e humanos) que compõem seu negócio. Afinal, o poder de proteção da corrente está diretamente associado ao elo mais fraco!

Em uma corporação, a segurança está ligada a tudo o que manipula direta ou indiretamente a informação (inclui-se aí também a própria informação e os usuários!!!), e que merece proteção. Esses elementos são chamados de **ativos**, e podem ser divididos em:

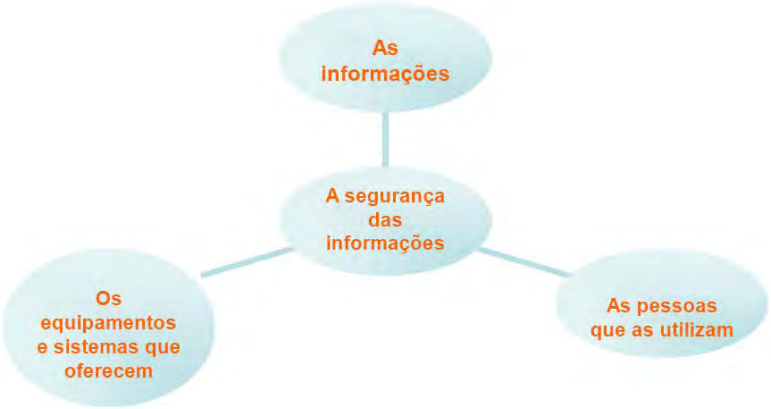
- tangíveis: informações impressas, móveis, hardware (Ex.:impressoras, *scanners*);
- intangíveis: marca de um produto, nome da empresa, confiabilidade de um órgão federal etc.;
- lógicos: informações armazenadas em uma rede, sistema ERP (sistema de gestão integrada) etc.;
- físicos: galpão, sistema de eletricidade, estação de trabalho etc.;
- humanos: funcionários.

Os ativos são os elementos que sustentam a operação do negócio e estes sempre trarão consigo VULNERABILIDADES que, por sua vez, submetem os ativos a AMEAÇAS.

Quanto maior for a organização maior será sua dependência com relação à informação, que pode estar armazenada de várias formas: impressa em papel, em meios digitais (discos, fitas, DVDs, disquetes, etc.), na mente das pessoas, em imagens armazenadas em fotografias/filmes...

Nesse sentido, é propósito da segurança proteger os elementos que fazem parte da comunicação, são eles:

- as informações;
- os equipamentos e sistemas que oferecem suporte a elas;
- as pessoas que as utilizam.



Elementos que a Segurança da Informação Busca Proteger

Princípios de segurança da informação

Ao estudarmos o tema, deparamo-nos com alguns princípios norteadores, segundo os padrões internacionais. Dentre estes princípios, podemos destacar a tríade **CID – Confidencialidade, Integridade** e **Disponibilidade.** Estes três atributos orientam a análise, o planejamento e a implementação da segurança da informação nas organizações.

Segundo a norma ABNT-ISO-IEC 27001, "adicionalmente outras propriedades, tais como **autenticidade, responsabilidade, não repúdio e confiabilidade**, podem também estar envolvidas". Estudemos, primeiramente, as três propriedades que fazem parte do conceito de segurança da informação.

Confidencialidade: preocupa-se com quem acessa as informações. Dizemos que existe confidencialidade quando somente as pessoas autorizadas possuem acesso à informação. Quando contamos um segredo a alguém - fazemos uma confidência - estamos dando acesso à informação. Mas não queremos que outras pessoas tenham acesso ao segredo, exceto à pessoa a quem estamos contando. Em outras palavras, a confidencialidade protege as informações de uma eventual revelação a alguém não autorizado. Observe que esta proteção não se aplica apenas à informação em sua forma digital; aplica-se a quaisquer mídias onde a informação esteja armazenada: CD, DVD, mídia impressa, entre outros. Além disso, nem mesmo uma pequena parte da informação poderá ser violada. A informação deve ser completamente protegida contra acessos indevidos. Se pensarmos, como exemplo, na Internet, onde os dados trafegam por vários caminhos e passam por diversas redes de computadores até chegarem ao destino, a confidencialidade deve garantir que os dados não serão vistos nem copiados por agentes não autorizados durante todo o percurso que realizarem na grande rede mundial.

Integridade: a informação deve manter todas as características originais durante sua existência. Estas características originais são as estabelecidas pelo proprietário da informação quando da criação ou manutenção da informação (se a informação for alterada por quem possui tal direito, isso não invalida a integridade). Existem vários exemplos de ataques feitos à integridade da informação: alteração em mensagens que trafegam na rede; modificação de *sites* da Internet; substituição de textos impressos ou em mídia digital etc.

Em resumo, a Integridade é o princípio da proteção da informação contra a criação ou modificação não autorizada. A violação da integridade pode estar relacionada com erro humano, por atos dolosos ou não. Esta violação pode tornar a informação sem valor ou, até, perigosa, especialmente se a violação for uma alteração da informação, o que pode levar a decisões equivocadas e causadoras de prejuízos.

Disponibilidade: garante que a informação esteja sempre disponível quando um usuário autorizado quiser acessar. A informação está lá quando for necessário recuperá-la. Claro que não consiste em uma violação da disponibilidade as interrupções dos serviços de acesso de forma autorizada ou programada, como nos casos de manutenção preventiva do sistema. A disponibilidade aplica-se à informação e aos canais de acesso a ela.

Veja o quadro abaixo. Resumimos os três princípios básicos em segurança da informação.

Segurança da Informação		
Princípio básico	**Conceito**	**Objetivo**
Confidencialidade	Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados	Proteger contra o acesso não autorizado, mesmo para dados em trânsito.
Integridade	Propriedade de salvaguarda da exatidão e completeza de ativos	Proteger informação contra modificação sem permissão; garantir a fidedignidade das informações.
Disponibilidade	Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada	Proteger contra indisponibilidade dos serviços (ou degradação); garantir aos usuários com autorização, o acesso aos dados.

O que a segurança da informação pretende é **diminuir o risco de sofrer qualquer perda do valor da informação**. A ideia é **evitar a ocorrência de incidentes de segurança da informação** que, segundo a ABNT, é "*um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação*".

Já um evento é "uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação".

Para a norma ISO 27001, um risco para a segurança da informação é uma combinação de fatores. De um modo geral, é a combinação de uma ameaça (temos aqui um agente) e uma vulnerabilidade (temos aqui uma fraqueza). Daí, combinando um agente com uma fraqueza, temos o **risco**. É um conceito mais geral para a idéia de risco.

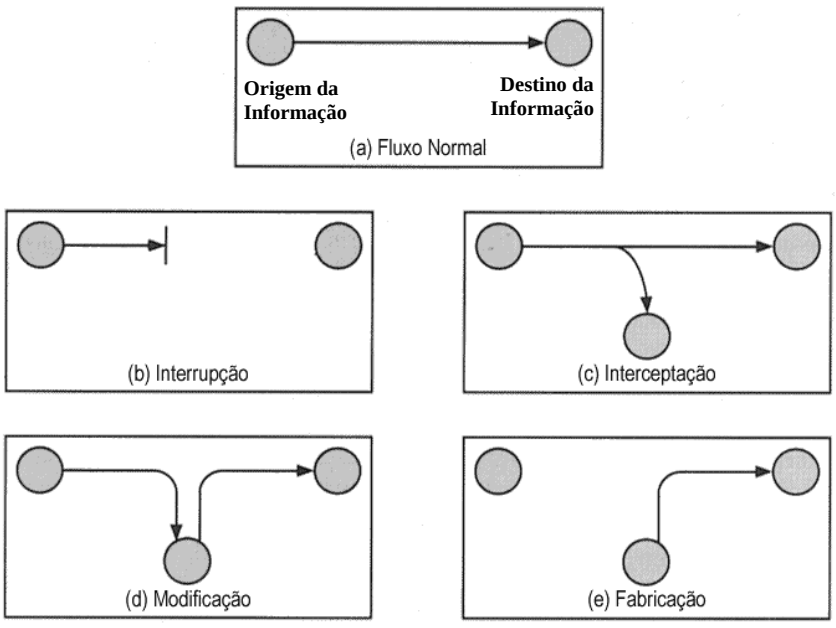
Cuidado para não pensar que as vulnerabilidades são apenas ligadas aos sistemas de informação em si. Lembre-se que existem os aspectos físicos e os aspectos lógicos. Existem os acontecimentos naturais que podem resultar em incidentes de segurança: incêndio, terremotos, inundações etc. Sem esquecermos dos incidentes com causa humana: negligência, imperícia, imprudência, vingança, terrorismo etc.; e, claro de fatos puramente técnicos: equipamentos com defeito, ruídos etc.

Nesse sentido, uma ameaça é qualquer coisa que possa afetar a operação, a disponibilidade, a integridade da informação. **Uma ameaça busca explorar uma vulnerabilidade – fraqueza – por meio de um ataque (técnica para explorar a vulnerabilidade).**

Do outro lado estão as contramedidas ou os mecanismos de defesa, que são as técnicas para defesa contra os ataques ou para reduzir as vulnerabilidades.

As principais origens das vulnerabilidades residem em falhas de projeto de hardware ou software, falhas na implantação (configuração errada, falta de treinamento), falhas de gerenciamento (problemas de monitoramento, procedimentos inadequados ou incorretos).

Observe a figura a seguir. Ela mostra alguns tipos de ataques em ambientes computacionais.



O fluxo normal da informação é o exemplificado em (a). Os demais exemplos mostram ataques realizados. Em (b) o fluxo é interrompido e o destinatário não recebe a mensagem. Diferentemente de (c), onde o receptor obtém a mensagem, mas há uma interceptação não autorizada. Em (d) e (e) o resultado é semelhante, pois o destinatário recebe uma mensagem diferente da original, sendo que em (d) houve uma modificação e em (e) uma mensagem nova foi encaminhada, com se fosse o remetente que a tivesse enviado.

Assim, temos:
(b) ➔ ataque à disponibilidade
(c) ➔ ataque à confidencialidade
(d) ➔ ataque à Integridade
(e) ➔ ataque à autenticidade

Vamos às questões!!

-LISTA DAS QUESTÕES COMENTADAS-

1. **(FGV/2010/SEFAZ-RJ/Fiscal de Rendas)** A assinatura digital visa dar garantia de integridade e autenticidade a arquivos eletrônicos, comprova que a mensagem ou arquivo não foi alterado e que foi assinado pela entidade ou pessoa que possui a chave privada e o certificado digital correspondente, utilizados na assinatura.
   A assinatura digital emprega chaves criptográficas definidas como um conjunto de bits baseado em um determinado algoritmo capaz de

cifrar e decifrar informações que, para isso, utiliza chaves simétricas ou chaves assimétricas. A esse respeito, analise as afirmativas a seguir.

I. Chaves simétricas são simples e nelas o emissor e o receptor utilizam a mesma chave para cifrar e decifrar uma informação, acarretando riscos menores, diminuindo consideravelmente as possibilidades de extravio ou fraudes. É por esta razão que chaves públicas são utilizadas em assinaturas digitais.

II. Chaves assimétricas funcionam com duas chaves: a chave privada e a chave pública. Nesse esquema, uma pessoa ou uma organização deve utilizar uma chave de codificação e disponibilizá-la a quem for mandar informações a ela. Essa é a chave pública. Uma outra chave deve ser usada pelo receptor da informação para o processo de decodificação: é a chave privada, que é sigilosa e individual. As chaves são geradas de forma conjunta, portanto, uma está associada à outra.

III. A assinatura digital funciona da seguinte forma: é necessário que o emissor tenha um documento eletrônico e a chave pública do destinatário. Por meio de algoritmos apropriados, o documento é então cifrado de acordo com esta chave pública. O receptor usará então sua chave privada correspondente para decifrar o documento. Se qualquer bit deste for alterado, a assinatura será deformada, invalidando o arquivo.

Assinale:

a) se somente a afirmativa I estiver correta.

b) se somente as afirmativas I e II estiverem corretas.

c) se somente as afirmativas I e III estiverem corretas.

d) se somente as afirmativas II e III estiverem corretas.

e) se todas as afirmativas estiverem corretas.

Resolução

Vamos relembrar os conceitos de chaves simétricas e assimétricas antes de resolver a questão.

Chave simétrica

Esse é um tipo de chave mais simples, em que o emissor e o receptor fazem uso da mesma chave, isto é, **UMA** única chave é usada na codificação e na decodificação da informação.

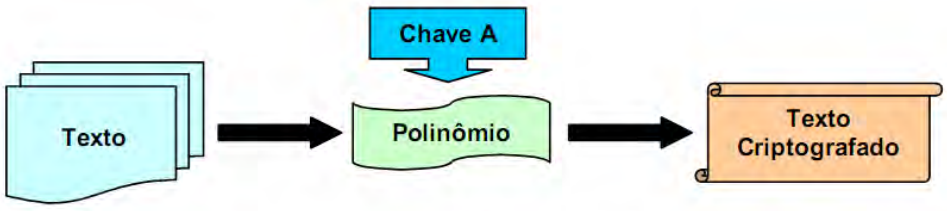


Figura 1 – Criptografia Simétrica – Encriptar

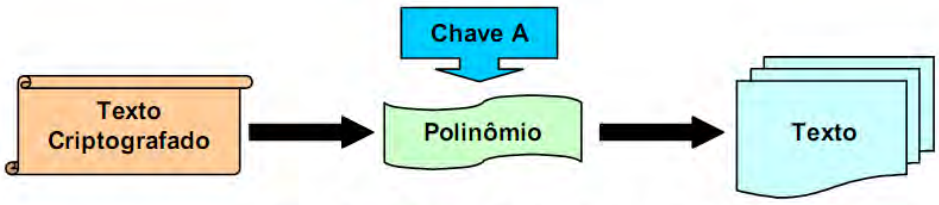


Figura 2 – Criptografia Simétrica – Decriptar

Nas figuras acima, podemos observar o funcionamento da criptografia simétrica. Uma informação é encriptada através de um polinômio utilizando-se de uma chave (Chave A) que também serve para decriptar a informação.

As principais vantagens dos **algoritmos simétricos** são:

- rapidez: um polinômio simétrico encripta um texto longo em milésimos de segundos;
- chaves pequenas: uma chave de criptografia de 128 bits torna um algoritmo simétrico praticamente impossível de ser quebrado.

A maior desvantagem da criptografia simétrica é que a chave utilizada para encriptar é igual à chave que decripta. Quando um grande número de pessoas tem conhecimento da chave, a informação deixa de ser um segredo.

O uso de chaves simétricas tem algumas desvantagens, fazendo com que sua utilização não seja adequada em situações em que a informação é muito valiosa. Para começar, é necessário usar uma grande quantidade de chaves caso muitas pessoas estejam envolvidas.

Ainda, há o fato de que tanto o emissor quanto o receptor precisa conhecer a chave usada. A transmissão dessa chave de um para o outro pode não ser tão segura e cair em "mãos erradas".

Chave assimétrica

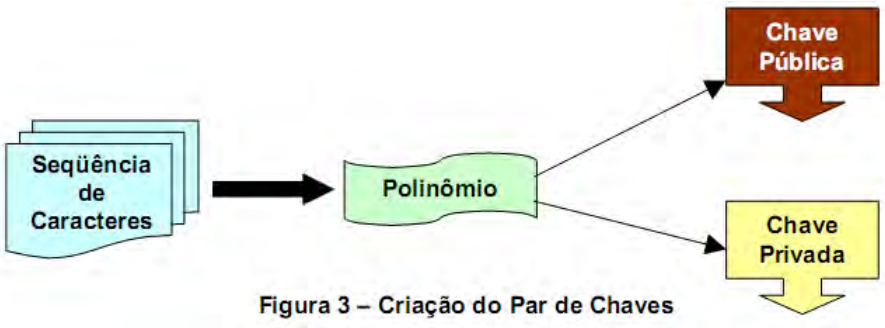


Figura 3 – Criação do Par de Chaves

Também conhecida como "chave pública", a técnica de criptografia por chave assimétrica trabalha com **DUAS** chaves: uma denominada privada

e outra denominada pública. Nesse método, uma pessoa deve criar uma chave de codificação e enviá-la a quem for mandar informações a ela. Essa é a chave pública. Outra chave deve ser criada para a decodificação. Esta – a chave privada – é secreta.

Para entender melhor, imagine o seguinte: o USUÁRIO-A criou uma chave pública e a enviou a vários outros sites. Quando qualquer desses sites quiser enviar uma informação criptografada ao USUÁRIO-A deverá utilizar a chave pública deste. Quando o USUÁRIO-A receber a informação, apenas será possível extraí-la com o uso da chave privada, que só o USUÁRIO-A tem. Caso o USUÁRIO-A queira enviar uma informação criptografada a outro site, deverá conhecer sua chave pública.

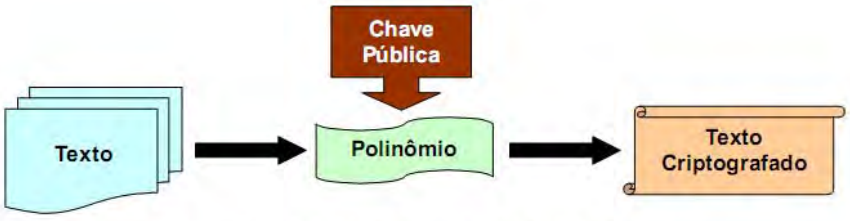


Figura 4 – Criptografia Assimétrica – Encriptar

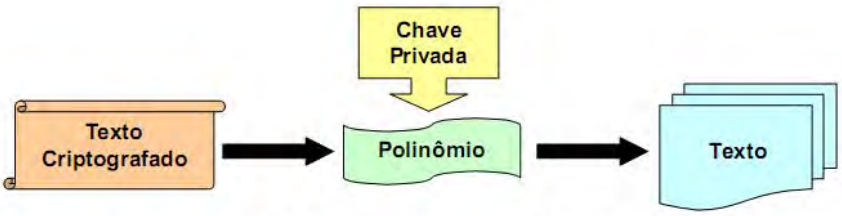


Figura 5 – Criptografia Assimétrica – Decriptar

Voltando à questão:

O item I está errado porque afirma que os riscos são menores ao se utilizar chaves simétricas, o que não é verdade. Como existe apenas uma chave,

ela deverá ser conhecida por todos os destinatários, aumentando o risco de extravio ou fraudes.

GABARITO: letra D.

2. **(FGV/2008/SEFAZ-RJ/Fiscal de Rendas)** Analise a citação abaixo, relacionada às fraudes na Internet.

"*Como se não bastassem vírus e spam, agora, os internautas têm que ficar atentos para outro tipo de ameaça: as fraudes online. A prática é sempre a mesma: um e-mail chega à Caixa de Entrada do programa de correio eletrônico oferecendo promoções e vantagens, ou solicitando algum tipo de recadastramento. A isca para "pescar" os usuários são empresas conhecidas, como bancos, editoras de jornais e revistas, e lojas de comércio eletrônico.*

Os golpes são bem elaborados, mas basta um pouco de atenção para verificar uma série de incoerências. Em geral, as mensagens são similares às originais enviadas pelas empresas, e muitas delas têm links para sites que também são cópias dos verdadeiros.

Mas, nos dois casos, é possível ver imagens quebradas, textos fora de formatação e erros de português - algo difícil de ocorrer com empresas que investem tanto em marketing para atrair clientes. Bom... e o que esses fraudadores querem, afinal?

Em alguns casos, o propósito é fazer o internauta preencher um formulário no site falso, enviando informações pessoais. Outras mensagens pedem apenas que o usuário baixe um arquivo − por exemplo, um suposto questionário − que, na verdade, é um programa que envia os dados pessoais e financeiros por meio da

Internet. De qualquer forma, é bom ficar de olho na sua Caixa de Entrada."

A citação caracteriza o uso de um tipo de fraude na Internet conhecido por:

(A) Keylogger Malware
(B) Denial of Service
(C) Hoax Spammer
(D) Phishing Scam
(E) Trojan Horse

Resolução

Esta questão destaca o **Golpe de *Phishing Scam*** (ou simplesmente Golpe de ***Phishing***), muito cobrado nas provas de concursos!

*O **Phishing*** (ou ***Phishing scam***) foi um termo criado para descrever o tipo de **fraude** que se dá através do **envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, como um banco, órgão do governo** (Receita Federal, INSS e Ministério do Trabalho são os mais comuns) **ou *site* popular, e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários desavisados.**

A Figura 6 listada a seguir apresenta uma "isca" (*e-mail*) envolvendo o Banco do Brasil bastante utilizada em golpes de *phishing.*

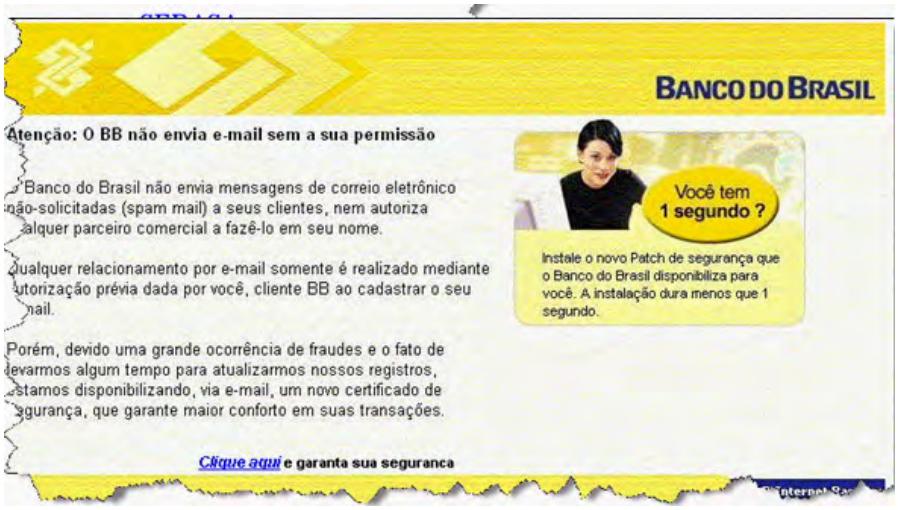


Figura 6. Isca de *Phishing* Relacionada ao Banco do Brasil

A palavra ***phishing*** (de *fishing*) vem de uma analogia criada pelos fraudadores, em que **"iscas" (*e-mails*) são usadas para "pescar" informações sensíveis (senhas e dados financeiros, por exemplo) de usuários da Internet**.

Atualmente, este termo vem sendo utilizado também para se referir aos seguintes casos:

- mensagem que procura induzir o usuário à instalação de códigos maliciosos, projetados para furtar dados pessoais e financeiros;
- mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros de usuários.

O objetivo principal de um *scammer* (indivíduo que implementa o Golpe de *Phishing Scam*) é **obter a autenticação**. Isto quer dizer, reunir as informações necessárias para se fazer passar pela VÍTIMA e obter alguma vantagem financeira. Em seguida, após obter os dados do cartão de crédito, fazer compras pela Internet; após obter os dados da conta

corrente ou poupança, fazer compras *on-line*, pagamentos ou transferências; dentre outros.

A Figura 7 ilustra alguns dos temas mais explorados pelos *scammers*.

Figura 7. Temas mais explorados pelos *Scammers* no Golpe de *Phishing Scam*

GABARITO: letra D.

3. **(FGV/2008/SEFAZ-RJ/Fiscal de Rendas)** Analise os casos descritos a seguir, referentes a fraudes envolvendo o comércio eletrônico e Internet Banking.

   I. O usuário recebe um *e-mail* de um suposto funcionário da instituição que mantém o *site* de comércio eletrônico ou de um banco, que persuade o usuário a fornecer informações sensíveis, como senhas de acesso ou número de cartões de crédito.

   II. Um *hacker* compromete o DNS do provedor do usuário, de modo que todos os acessos a um *site* de comércio eletrônico ou *Internet Banking*

são redirecionados para uma página Web falsificada, semelhante ao *site* verdadeiro, com o objetivo de o atacante monitorar todas as ações do usuário, como a digitação de sua senha bancária. Nesta situação, normalmente o usuário deve aceitar um novo certificado (que não corresponde ao *site* verdadeiro), e o endereço mostrado no *browser* do usuário é diferente do endereço correspondente ao *site* verdadeiro.

III. O usuário recebe um *e-mail*, cujo remetente é o gerente do seu banco e que contém uma mensagem que solicita a execução pelo usuário de um programa anexo ao *e-mail* recebido, a título de obter acesso mais rápido às informações mais detalhadas em sua conta bancária.

IV. O usuário utiliza computadores de terceiros para acessar *sites* de comércio eletrônico ou de *Internet Banking*, possibilitando o monitoramento de suas ações, incluindo a digitação de senhas ou número de cartões de crédito, por meio de programas especificamente projetados para esse fim.

Constituem exemplos de fraudes resultantes de Engenharia Social os casos identificados em:

(A) I e II.

(B) I e III.

(C) II e III.

(D) II e IV.

(E) III e IV.

Resolução

Engenharia Social é uma técnica em que o atacante (se fazendo passar por outra pessoa) utiliza-se de meios, como uma ligação telefônica ou *e-mail*, para PERSUADIR o usuário a fornecer informações ou realizar determinadas ações.

Exemplo: algum desconhecido liga para a sua casa e diz ser do suporte técnico do seu provedor de acesso. Nesta ligação ele informa que sua conexão com a Internet está apresentando algum problema e, então, solicita sua senha para corrigi-lo. Caso a senha seja fornecida por você, este "suposto técnico" poderá realizar uma infinidade de atividades maliciosas com a sua conta de acesso à Internet e, portanto, relacionando tais atividades ao seu nome.

Vamos à resolução da questão:

Item I. A descrição envolve o uso da **engenharia social**, já que alguém (via *e-mail* neste caso, poderia ser por telefone!) faz uso da persuasão, da ingenuidade ou confiança do usuário, para obter informações como número do cartão de crédito e senha do usuário. O item I é **VERDADEIRO**.

Item II. Nesse caso, como não houve contato entre o *hacker* e a vítima, o golpe não pode ser configurado como engenharia social. O golpe em destaque é intitulado ***Pharming*** (também conhecido como ***DNS Poisoining*** - "**envenamento de DNS**"). O item II é **FALSO**.

É isso mesmo pessoal!! Muita atenção neste tipo de golpe! O enunciado do item II o descreve claramente, e gostaríamos de complementar ☺....

O **Pharming** é um tipo de golpe bem mais elaborado que o *Phishing*, pois envolve algum tipo de redirecionamento da vítima para *sites* fraudulentos, através de alterações nos serviços de resolução de nomes (DNS).

Lembre-se de que **no Pharming o servidor DNS do provedor do usuário é comprometido**, de modo que todos os acessos a um *site* de comércio eletrônico ou Internet Banking são redirecionados para uma página Web falsificada, semelhante ao *site* verdadeiro, com o objetivo de o atacante monitorar todas as ações do usuário, como a digitação de sua senha bancária.

Exemplo: pode envolver alteração, no servidor DNS, do endereço IP associado ao endereço www.bradesco.com.br para que aponte para um *site* réplica do banco Bradesco.

Item III. Novamente, o usuário recebe uma mensagem do suposto gerente do banco, induzindo-o a executar um programa qualquer. O item III é **VERDADEIRO**.

Item IV. Não há engenharia social neste caso. O item IV é **FALSO**.

GABARITO: letra B.

Você Sabia!!! Qual diferença entre *Crackers* e *Hackers*? Um é do bem e o outro do mal?

O termo ***hacker*** ganhou, junto à opinião pública influenciada pelos meios de comunicação, uma conotação negativa, que nem sempre corresponde à realidade!!

Os ***hackers***, por sua definição geral, são aqueles que utilizam seus conhecimentos para invadir sistemas, não com o intuito de causar danos às vítimas, mas sim como um desafio às suas habilidades. Eles invadem os sistemas, capturam ou modificam arquivos para provar sua capacidade e depois compartilham suas proezas com os colegas. Eles não têm a intenção de prejudicar, mas sim de apenas demonstrar que conhecimento é poder.

Exímios programadores e conhecedores dos segredos que envolvem as redes e os computadores, eles geralmente não gostam de ser confundidos com *crackers*.

Os ***crackers*** são elementos que invadem sistemas para roubar informações e causar danos às vítimas. O termo *crackers* também é uma denominação utilizada para aqueles que decifram códigos e destroem proteções de software.

Atualmente, a imprensa mundial atribui qualquer incidente de segurança a hackers, em seu sentido genérico. A palavra *cracker* não é vista nas reportagens, a não ser como *cracker* de senhas, que é um software utilizado para descobrir senhas ou decifrar mensagens cifradas.

4. **(FUNRIO/2009/Analista de Seguro Social/Serviço Social)** 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 troia são alguns dos exemplos de *Malware*.

Estão corretas:

A) I, II e III, apenas.

B) I e IV, apenas.

C) II e IV, apenas.

D) III e IV, apenas.

E) I, II, III e IV.

Resolução

Item I. A **Criptografia** é a ciência e arte de escrever mensagens em forma cifrada ou em código. Os métodos de criptografia atuais são seguros e eficientes e baseiam-se no uso de uma ou mais chaves. A chave é uma sequência de caracteres, que pode conter letras, dígitos e símbolos (como uma senha), e que é convertida em um número, utilizado pelos métodos de criptografia para codificar e decodificar mensagens.

Atualmente, os métodos criptográficos podem ser subdivididos em duas grandes categorias, de acordo com o tipo de chave utilizada: a criptografia de chave única e a criptografia de chave pública e privada.

- A **criptografia de chave única** utiliza a **MESMA** chave tanto para codificar quanto para decodificar mensagens.

- A **criptografia de chaves pública e privada** utiliza **DUAS** chaves distintas, uma para codificar e outra para decodificar mensagens. Neste método cada pessoa ou entidade mantém duas chaves: uma pública, que pode ser divulgada livremente, e outra privada, que deve ser mantida

em segredo pelo seu dono. As mensagens codificadas com a chave pública só podem ser decodificadas com a chave privada correspondente.

Cabe destacar que a principal finalidade da criptografia é, sem dúvida, reescrever uma mensagem original de uma forma que seja incompreensível, para que ela não seja lida por pessoas não-autorizadas. E isso não é suficiente para impedir a invasão de redes. Item **FALSO**.

Item II. O **certificado digital** é uma credencial eletrônica, não-palpável gerada por uma Autoridade Certificadora (**AC**), que vincula a pessoa física ou jurídica a um par de chaves sendo uma pública e outra privada (ou secreta). O certificado fica armazenado em dispositivos de segurança, como por ex.: *Token* ou *Smart Card*, ilustrados na figura seguinte.

Token

Smart Card

Figura 8. Ilustração de dispositivos de segurança

Quanto aos objetivos do certificado digital podemos destacar:

- Transferir a credibilidade que hoje é baseada em papel e conhecimento para o ambiente eletrônico.
- **Vincular uma chave pública a um titular** (eis o objetivo principal). O certificado digital precisa ser emitido por uma autoridade reconhecida pelas partes interessadas na transação, conforme visto na próxima figura 9. Chamamos essa autoridade de **Autoridade Certificadora**, ou **AC**.

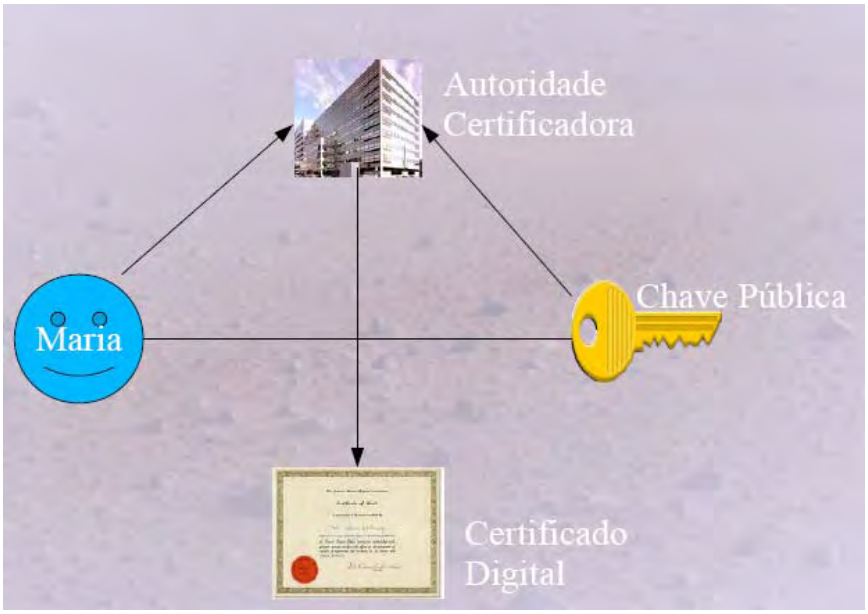
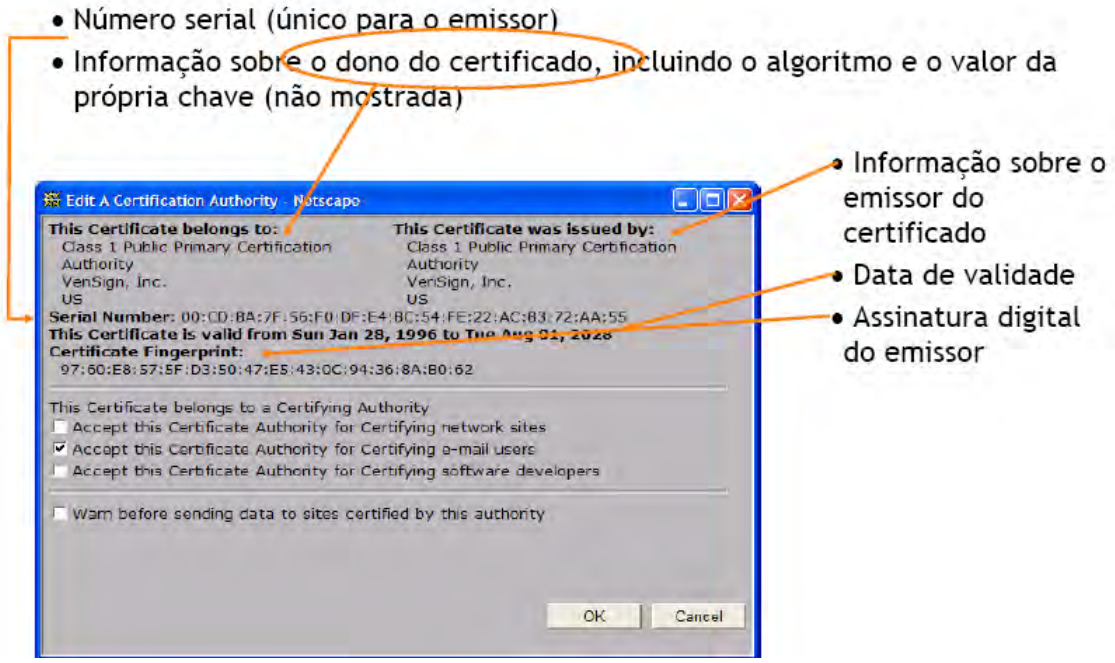


Figura 9. Vínculo da chave pública ao titular

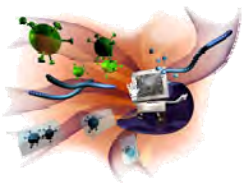
Um certificado contém:



Item **VERDADEIRO**.

A seguir, iremos explicar primeiramente o item IV, em seguida, passamos aos comentários do item III, para uma melhor compreensão.

Item IV. **O que significa *malware*?**



Malware é proveniente de ***Malicious Software***, software designado a se infiltrar em um sistema de computador alheio de forma ilícita com o intuito de causar algum dano ou roubo de informações. Também pode ser considerado *malware* uma aplicação legal que por uma falha de programação (intencional ou não) execute funções que se enquadrem na definição.

Resumindo, ***malwares* são programas que executam deliberadamente ações mal-intencionadas em um computador**!!

Uma dica: caso tenha condições de baixar alguns vídeos da Internet, no site **http://www.antispam.br/videos/** são disponibilizados os vídeos do CertBr que ilustram de forma bem didática a diferença entre os diversos tipos de *malware* (como vírus, worms, screenloggers, etc), bem como os mecanismos de defesa principais contra as ameaças da Internet. É uma boa fonte de informação para todos vocês!!! Aproveitem!!

Os tipos mais comuns de *malware:* vírus, *worms*, bots, cavalos de troia, *spyware*, *keylogger*, *screenlogger*, estão descritos a seguir.

- **Vírus**: são pequenos códigos de programação maliciosos que se "agregam" a arquivos e são transmitidos com eles. Quando o arquivo é aberto na memória RAM, o vírus também é, e, a partir daí se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção. Alguns vírus são inofensivos, outros, porém, podem danificar um sistema operacional e os programas de um computador.
- ***Worms***: são programas parecidos com vírus, mas que na verdade são capazes de se propagarem automaticamente através de redes, enviando cópias de si mesmo de computador para computador (observe que os *worms* apenas se copiam, não infectam outros arquivos, eles mesmos são os arquivos!!). Além disso, geralmente utilizam as redes de comunicação para infectar outros computadores (via *e-mails*, Web, FTP, redes das empresas, etc.).

Diferentemente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da

exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

- **Bots**: de modo similar ao *worm*, é um programa capaz se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de software instalado em um computador. Adicionalmente ao *worm*, dispõe de mecanismos de comunicação com o invasor, permitindo que o bot seja controlado remotamente.
- ***Trojan horse* (Cavalo de troia)**: é um programa aparentemente inofensivo que entra em seu computador na forma de cartão virtual, álbum de fotos, protetor de tela, jogo, etc., e que, quando executado (com a sua autorização!), parece lhe divertir, mas, por trás abre portas de comunicação do seu computador para que ele possa ser invadido. Por definição, o cavalo de troia distingue-se de um vírus ou de um *worm* por não infectar outros arquivos, nem propagar cópias de si mesmo automaticamente.

  O *trojans* ficaram famosos na Internet pela facilidade de uso, e por permitirem a qualquer pessoa possuir o controle de um outro computador apenas com o envio de um arquivo.

  Os *trojans* atuais são divididos em duas partes, que são: o servidor e o cliente. Normalmente, o servidor encontra-se oculto em algum outro arquivo e, no momento em que o arquivo é executado, o servidor se instala e se oculta no computador da vítima. Nesse momento, o computador já pode ser acessado pelo cliente, que enviará informações para o servidor executar certas operações no computador da vítima.
- ***Spyware*:** programa que tem por finalidade monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

- ***Keylogger***: um tipo de *malware* que é capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Dentre as informações capturadas podem estar o texto de um *e-mail*, dados digitados na declaração de Imposto de Renda e outras informações sensíveis, como senhas bancárias e números de cartões de crédito. Em muitos casos, a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um *site* específico de comércio eletrônico ou Internet Banking. Normalmente, o *keylogger* contém mecanismos que permitem o envio automático das informações capturadas para terceiros (por exemplo, através de *e-mails*).
- ***Screenlogger***: forma avançada de *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado.

Item **VERDADEIRO**.

Item III. Os antivírus procuram detectar e, então, anular ou remover códigos maliciosos do computador (vírus, vermes, cavalos de troia, etc.). Exs: McAfee Security Center Antivírus, Panda Antivírus, Norton Antivírus, Avira Antivir Personal, AVG, etc.

Ao contrário do que afirma a questão, **o antivírus não impede que um atacante explore alguma vulnerabilidade (fragilidade, ponto fraco) existente no computador.**

Algumas práticas são recomendadas na prevenção/detecção de *malware*, como:

- ter instalado, em seu computador e no da empresa, um programa antivírus capaz de detectar a presença de *malware* em *e-mails* ou arquivos do computador. Esse utilitário conta, muitas vezes, com a vacina capaz de "matar" o *malware* e deixar o arquivo infectado SEM a ameaça.

  Alguns fornecedores de programas antivírus distribuem atualizações regulares do seu produto. Muitos programas antivírus têm um recurso de atualização automática. Quando o programa antivírus é atualizado, informações sobre novos vírus são adicionadas a uma lista de vírus a serem verificados. Quando não possui a vacina, ele, pelo menos, tem como detectar o vírus, informando ao usuário acerca do perigo que está iminente;
- não executar ou abrir arquivos recebidos por *e-mail* ou por outras fontes, mesmo que venham de pessoas conhecidas (caso seja necessário abrir o arquivo, certifique-se de que ele foi verificado pelo programa antivírus);
- procurar utilizar na elaboração de documentos formatos menos suscetíveis à propagação de vírus, tais como RTF, ou PDF, dentre outros;
- não abrir arquivos anexos a *e-mails* de pessoas que você não conhece; idem para os *e-mails* de pessoas conhecidas também! (Os *Worms* atuais atacam um computador e usam a sua listagem de endereços para mandar um *e-mail* para cada pessoa da lista como se fosse o dono do computador!), etc.

Item **FALSO**.

GABARITO: letra C.

5. **(ESAF/2005/AFRFB)** Em relação a vírus de computador é correto afirmar que, entre as categorias de malware, o Cavalo de Troia é um programa que

a) usa um código desenvolvido com a expressa intenção de se replicar. Um Cavalo de Troia tenta se alastrar de computador para computador incorporando-se a um programa hospedeiro. Ele pode danificar o hardware, o software ou os dados. Quando o hospedeiro é executado, o código do Cavalo de Troia também é executado, infectando outros hospedeiros e, às vezes, entregando uma carga adicional.

b) pode ser executado e pode se alastrar sem a intervenção do usuário, enquanto alguns variantes desta categoria de malware exigem que os usuários executem diretamente o código do Cavalo de Troia para que eles se alastrem. Os Cavalos de Troia também podem entregar uma carga além de se replicarem.

c) usa um código mal-intencionado auto-propagável que pode se distribuir automaticamente de um computador para outro através das conexões de rede. Um Cavalo de Troia pode desempenhar ações nocivas, como consumir recursos da rede ou do sistema local, possivelmente causando um ataque de negação de serviço.

d) não pode ser considerado um vírus ou um verme de computador porque tem a característica especial de se propagar. Entretanto, um Cavalo de Troia pode ser usado para copiar um vírus ou um verme em um sistema-alvo como parte da carga do ataque, um processo conhecido como descarga. A intenção típica de um Cavalo de Troia é interromper o trabalho do usuário ou as operações normais do sistema.

Por exemplo, o Cavalo de Troia pode fornecer uma porta dos fundos no sistema para que um hacker roube dados ou altere as definições da configuração.

e) parece útil ou inofensivo, mas contém códigos ocultos desenvolvidos para explorar ou danificar o sistema no qual é executado. Os cavalos de troia geralmente chegam aos usuários através de mensagens de e-mail que disfarçam a finalidade e a função do programa. Um Cavalo de Troia faz isso entregando uma carga ou executando uma tarefa mal-intencionada quando é executado.

Resolução

Um cavalo de troia (*trojan horse*) é um programa "aparentemente" normal e inofensivo (jogo, *screen-saver*, etc.) que carrega dentro de si instruções que não são originalmente suas, inseridas com um propósito danoso, como:

- alteração ou destruição de arquivos;
- furto de senhas e outras informações sensíveis, como nº de cartões de crédito;
- inclusão de *backdoors*, para permitir que um atacante tenha total controle sobre o computador.

O cavalo de troia distingue-se de um vírus ou de um *worm* por não infectar outros arquivos, nem propagar cópias de si mesmo automaticamente!!!

(Lembre-se disso, vai ser útil para você em provas futuras!)

GABARITO: letra E.

CONSIDERAÇÕES FINAIS

Bem, chegamos ao final da nossa aula demonstrativa.

Esperamos vocês em breve.

Grande abraço, bons estudos e até o nosso próximo encontro!

Patrícia Quintão e Alexandre Lênin

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança –Código de Prática para a Gestão de Segurança da Informação (antiga 17799:2005).

CERTBR. Cartilha de Segurança para Internet. 2006.

RAMOS, A.; BASTOS, A.; LAYRA, A. **Guia oficial para formação de gestores em segurança da informação.** 1. ed. Rio Grande do Sul: ZOUK. 2006.

SÊMOLA, M. **Gestão da segurança da informação**. 2 ed. São Paulo: Campus Elsevier. 2003.

TECHNET. **Academia Latino-Americana da Segurança da Informação**. 2006. Disponível em: <http://www.technetbrasil.com.br/academia/>.

- LISTA DAS QUESTÕES APRESENTADAS NA AULA –

1. **(FGV/2010/SEFAZ-RJ/Fiscal de Rendas)** A assinatura digital visa dar garantia de integridade e autenticidade a arquivos eletrônicos, comprova que a mensagem ou arquivo não foi alterado e que foi assinado pela entidade ou pessoa que possui a chave privada e o certificado digital correspondente, utilizados na assinatura.

   A assinatura digital emprega chaves criptográficas definidas como um conjunto de bits baseado em um determinado algoritmo capaz de cifrar e decifrar informações que, para isso, utiliza chaves simétricas ou chaves assimétricas. A esse respeito, analise as afirmativas a seguir.

   I. Chaves simétricas são simples e nelas o emissor e o receptor utilizam a mesma chave para cifrar e decifrar uma informação, acarretando riscos menores, diminuindo consideravelmente as possibilidades de extravio ou fraudes. É por esta razão que chaves públicas são utilizadas em assinaturas digitais.

   II. Chaves assimétricas funcionam com duas chaves: a chave privada e a chave pública. Nesse esquema, uma pessoa ou uma organização deve utilizar uma chave de codificação e disponibilizá-la a quem for mandar informações a ela. Essa é a chave pública. Uma outra chave deve ser usada pelo receptor da informação para o processo de decodificação: é a chave privada, que é sigilosa e individual. As chaves são geradas de forma conjunta, portanto, uma está associada à outra.

   III. A assinatura digital funciona da seguinte forma: é necessário que o emissor tenha um documento eletrônico e a chave pública do destinatário. Por meio de algorítmos apropriados, o documento é então cifrado de acordo com esta chave pública. O receptor usará então sua

chave privada correspondente para decifrar o documento. Se qualquer bit deste for alterado, a assinatura será deformada, invalidando o arquivo.

Assinale:

a) se somente a afirmativa I estiver correta.

b) se somente as afirmativas I e II estiverem corretas.

c) se somente as afirmativas I e III estiverem corretas.

d) se somente as afirmativas II e III estiverem corretas.

e) se todas as afirmativas estiverem corretas.

2. **(FGV/2008/SEFAZ-RJ/Fiscal de Rendas)** Analise a citação abaixo, relacionada às fraudes na Internet.

"*Como se não bastassem vírus e spam, agora, os internautas têm que ficar atentos para outro tipo de ameaça: as fraudes online. A prática é sempre a mesma: um e-mail chega à Caixa de Entrada do programa de correio eletrônico oferecendo promoções e vantagens, ou solicitando algum tipo de recadastramento. A isca para "pescar" os usuários são empresas conhecidas, como bancos, editoras de jornais e revistas, e lojas de comércio eletrônico.*

Os golpes são bem elaborados, mas basta um pouco de atenção para verificar uma série de incoerências. Em geral, as mensagens são similares às originais enviadas pelas empresas, e muitas delas têm links para sites que também são cópias dos verdadeiros.

Mas, nos dois casos, é possível ver imagens quebradas, textos fora de formatação e erros de português - algo difícil de ocorrer com

empresas que investem tanto em marketing para atrair clientes. Bom... e o que esses fraudadores querem, afinal?

Em alguns casos, o propósito é fazer o internauta preencher um formulário no site falso, enviando informações pessoais. Outras mensagens pedem apenas que o usuário baixe um arquivo – por exemplo, um suposto questionário – que, na verdade, é um programa que envia os dados pessoais e financeiros por meio da Internet. De qualquer forma, é bom ficar de olho na sua Caixa de Entrada."

A citação caracteriza o uso de um tipo de fraude na Internet conhecido por:

(A) Keylogger Malware
(B) Denial of Service
(C) Hoax Spammer
(D) Phishing Scam
(E) Trojan Horse

3. **(FGV/2008/SEFAZ-RJ/Fiscal de Rendas)** Analise os casos descritos a seguir, referentes a fraudes envolvendo o comércio eletrônico e Internet Banking.

I. O usuário recebe um *e-mail* de um suposto funcionário da instituição que mantém o *site* de comércio eletrônico ou de um banco, que persuade o usuário a fornecer informações sensíveis, como senhas de acesso ou número de cartões de crédito.

II. Um *hacker* compromete o DNS do provedor do usuário, de modo que todos os acessos a um *site* de comércio eletrônico ou *Internet Banking*

são redirecionados para uma página Web falsificada, semelhante ao *site* verdadeiro, com o objetivo de o atacante monitorar todas as ações do usuário, como a digitação de sua senha bancária. Nesta situação, normalmente o usuário deve aceitar um novo certificado (que não corresponde ao *site* verdadeiro), e o endereço mostrado no *browser* do usuário é diferente do endereço correspondente ao *site* verdadeiro.

III. O usuário recebe um *e-mail*, cujo remetente é o gerente do seu banco e que contém uma mensagem que solicita a execução pelo usuário de um programa anexo ao *e-mail* recebido, a título de obter acesso mais rápido às informações mais detalhadas em sua conta bancária.

IV. O usuário utiliza computadores de terceiros para acessar *sites* de comércio eletrônico ou de *Internet Banking*, possibilitando o monitoramento de suas ações, incluindo a digitação de senhas ou número de cartões de crédito, por meio de programas especificamente projetados para esse fim.

Constituem exemplos de fraudes resultantes de Engenharia Social os casos identificados em:

(A) I e II.

(B) I e III.

(C) II e III.

(D) II e IV.

(E) III e IV.

4. **(FUNRIO/2009/Analista de Seguro Social – Serviço Social)** 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 troia são alguns dos exemplos de *Malware*.

Estão corretas:

A) I, II e III, apenas.

B) I e IV, apenas.

C) II e IV, apenas.

D) III e IV, apenas.

E) I, II, III e IV.

5. **(ESAF/2005/AFRFB)** Em relação a vírus de computador é correto afirmar que, entre as categorias de malware, o Cavalo de Troia é um programa que

a) usa um código desenvolvido com a expressa intenção de se replicar. Um Cavalo de Troia tenta se alastrar de computador para computador incorporando-se a um programa hospedeiro. Ele pode danificar o hardware, o software ou os dados. Quando o hospedeiro é executado, o código do Cavalo de Troia também é executado, infectando outros hospedeiros e, às vezes, entregando uma carga adicional.

b) pode ser executado e pode se alastrar sem a intervenção do usuário, enquanto alguns variantes desta categoria de malware exigem

que os usuários executem diretamente o código do Cavalo de Troia para que eles se alastrem. Os Cavalos de Troia também podem entregar uma carga além de se replicarem.

c) usa um código mal-intencionado auto-propagável que pode se distribuir automaticamente de um computador para outro através das conexões de rede. Um Cavalo de Troia pode desempenhar ações nocivas, como consumir recursos da rede ou do sistema local, possivelmente causando um ataque de negação de serviço.

d) não pode ser considerado um vírus ou um verme de computador porque tem a característica especial de se propagar. Entretanto, um Cavalo de Troia pode ser usado para copiar um vírus ou um verme em um sistema-alvo como parte da carga do ataque, um processo conhecido como descarga. A intenção típica de um Cavalo de Troia é interromper o trabalho do usuário ou as operações normais do sistema. Por exemplo, o Cavalo de Troia pode fornecer uma porta dos fundos no sistema para que um hacker roube dados ou altere as definições da configuração.

e) parece útil ou inofensivo, mas contém códigos ocultos desenvolvidos para explorar ou danificar o sistema no qual é executado. Os cavalos de troia geralmente chegam aos usuários através de mensagens de e-mail que disfarçam a finalidade e a função do programa. Um Cavalo de Troia faz isso entregando uma carga ou executando uma tarefa mal-intencionada quando é executado.

GABARITO

1. D.
2. D.
3. B.
4. C.
5. E.