

Melo, William da Silva

M528m pMOOC Segurança da Informação: teoria aliada à prática/ William da Silva Melo.

II, 112f.

Produto Educacional parte da dissertação intitulada “Modelo de Formação para Educação Profissional e Tecnológica Baseada em pMOOC: Uma experiência com segurança da informação” apresentada ao Programa de Pós-Graduação em Educação Profissional e Tecnológica ofertado pelo Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano (IF Sertão PE) / Campus Salgueiro, Salgueiro, PE, 2020.

* + 1. Segurança da Informação 2. pMOOC 3. Plano de ensino – segurança da informação 4. Formação I. Título

CDD 371.33

Ficha Catalográfica Elaborada pela Bibliotecária Naira Michelle Alves Pereira CRB 4/1891

**SUMÁRIO**

1. APRESENTAÇÃO 3
2. DIRETRIZES DO MODELO DE FORMAÇÃO 4
3. PLANO DE ENSINO - PMOOC SEGURANÇA DA INFORMAÇÃO: ALIANDO TEORIA E PRÁTICA 7

APRESENTAÇÃO

O produto educacional fruto da pesquisa intitulada: Modelo de Formação para Educação Profissional e Tecnológica Baseada em pMOOC: Uma experiência com segurança da informação, apresentado pelo mestrando William da Silva Melo, sob orientação de Francisco Kelsen de Oliveira no programa de Pós Graduação em Educação Profissional e Tecnológica, ofertado pelo Instituto Federal de Educação, Ciências e Tecnologia do Sertão Pernambucano, campus Salgueiro se encaixa na modalidade de sequência didática.

Trata-se de um curso on-line aberto e massivo na área de segurança da informação, que tem a peculiaridade de trabalhar aspectos práticos e desenvolver habilidades e conhecimentos no público do Ensino Médio Integrado ao técnico de informática. Sendo assim, o pMOOC Segurança da Informação: Aliando teoria e prática foi desenvolvido com base no modelo de formação, construído nesta pesquisa, está disponível para acesso na plataforma Course Builder da Google (Link: <https://mooc-seginfo.appspot.com/moocseg/course>).

O pMOOC Segurança da Informação: Aliando teoria e prática possui carga horária de 40 horas, foi dividido em três unidades e utilizou os elementos demonstrados na figura 1. O período de aplicação do curso foi de 30 dias, a rede social Whatsapp foi utilizada como grupo de interação, o que permitiu tutoria em grupo individual para os alunos.

**Figura 1: Elementos do pMOOC**



Fonte: Elaborado pelo autor.

DIRETRIZES DO MODELO DE FORMAÇÃO

Para que o produto educacional pMOOC Segurança da Informação: Aliando Teoria e Prática possa ser adaptado para outras áreas do conhecimento, educadores poderão se basear nos resultados e discussões feitas na pesquisa Modelo de Formação para Educação Profissional e Tecnológica Baseada em pMOOC: Uma experiência com segurança da informação. Além disso, podem ter como base as diretrizes baseadas nas perspectivas pedagógicas, tecnológicas e contextuais, conforme mostram os quadros 1, 2 e 3 abaixo.

**Quadro 1 - Perspectiva pedagógica do pMOOC**

|  |  |
| --- | --- |
| **ID** | **Diretrizes Pedagógicas** |
| PP1 | É necessário ter tutor/professor especializado na área para dar assistência aos alunos do curso. |
| PP2 | É necessário assistência do tutor/professor de forma on-line. |
| PP3 | É necessário que o plano de ensino contemple encontros presenciais com professor especializado na área. |
| PP4 | É necessário considerar uma abordagem introdutória sobre o conteúdo abordado no curso. |
| PP5 | Os objetivos instrucionais do curso devem seguir uma ordem crescente de complexidade, com base na taxonomia de Bloom. |
| PP6 | A abrangência do conteúdo deve seguir uma abordagem de básica a intermediária. |
| PP7 | É necessário aproximar o conteúdo da realidade do aluno, trazendo exemplo reais de situações alinhadas com os assuntos abordados. |
| PP8 | Devem ser utilizados métodos de avaliação diversificados. |
| PP9 | É necessário que os métodos de avaliação abordem questões teóricas e práticas. |
| PP10 | As atividades propostas devem evoluir em sua complexidade do nível básico para intermediário. |
| PP11 | Os desafios práticos devem abordar questões atuais, interessantes para o aluno e que possam ser aplicados em situações diferentes das abordadas no conteúdo |
| PP12 | Devem ser utilizadas metodologias ativas de ensino aprendizagem. |
| PP13 | Os alunos devem aplicar de modo prático o conhecimento adquirido no curso. |
| PP14 | Os jogos em grupo devem fazer parte do plano de ensino do curso. |

|  |  |
| --- | --- |
| PP15 | Os Conteúdos avançados devem ser abordados pelo tutor de maneira síncrona e interativa. |

Fonte: elaborado pelo autor.

**Quadro 2 - Perspectiva contextual do pMOOC**

|  |  |
| --- | --- |
| **ID** | **Diretrizes Contextuais** |
| PC1 | Se faz necessário um método de acompanhamento da evolução dos alunos no MOOC. |
| PC2 | É necessário utilizar estratégias para motivar o aluno a se dedicar ao curso. |
| PC3 | O plano de estudos definido para o curso não deve comprometer mais do que 60 minutos diários do tempo do aluno. |
| PC4 | Na elaboração do curso devem ser levados em consideração aspectos como expectativa de formação e interesse nos temas abordados para MOOC. |
| PC5 | Os estudantes devem ser familiarizados com o formato do curso. |
| PC6 | É necessário contextualizar o conteúdo com o mundo do trabalho. |
| PC7 | A comunidade acadêmica deve ser consultada sobre os conteúdos abordados no curso, a fim de garantir interesse dos alunos. |
| PC8 | O conteúdo textual deve ser consistente deixando claros os conceitos envolvidos nas práticas realizadas. |
| PC9 | O curso deve ter uma regularidade nas atividades propostas. |
| PC10 | As redes sociais podem ser utilizadas para interagir, questionar, motivar e alertar os alunos sobre questões relativas ao curso. |
| PC11 | Gratificar o aluno com pontuação extra estimula sua adesão ao curso. |
| PC12 | Os estudos de caso devem representar situações práticas que envolvam o cotidiano do mundo do trabalho. |
| PC13 | O cronograma deve fixar claramente prazos de início, datas de entregas de atividades e final do curso. |
| PC14 | O período ideal para aplicar um curso on-line na turma do médio integrado varia conforme a evolução da turma. |

Fonte: elaborado pelo autor.

**Quadro 3 - Perspectiva tecnológica do pMOOC**

|  |  |
| --- | --- |
| **ID** | **Diretrizes Tecnológicas** |
| PT1 | É necessário fornecer acesso aos recursos de TDICs do campus para possibilitar aos alunos oportunidade de realização do curso. |
| PT2 | O uso de TDICs é incentivado visto que, os alunos estão familiarizados em utilizar essas ferramentas, as mesmas são aliadas no processo de ensino/aprendizagem. |

|  |  |
| --- | --- |
| PT3 | Os alunos não estão familiarizados com fóruns de discussão, por outro lado é incentivada a utilização de rede social como ferramenta para comunicação em grupo. |
| PT4 | A plataforma utilizada para hospedar o curso deve ter boa usabilidade (fácil, intuitiva para utilizar). |
| PT5 | Devem ser utilizadas uma diversidade de mídias interativas e digitais tais como: Vídeos, animações, textos e imagens. |
| PT6 | A multimídia e as redes sociais devem apoiar o processo de ensino/aprendizado. |
| PT7 | As mídias utilizadas devem ser dinâmicas e interativas. |

Fonte: elaborado pelo autor.

PLANO DE ENSINO - pMOOC SEGURANÇA DA INFORMAÇÃO: ALIANDO TEORIA E PRÁTICA

1. Apresentação da plataforma e do curso (momento presencial)
2. Aplicação do jogo MOOCSEG (momento presencial)
3. Pré-teste
4. Unidade 1 - Introdução
   1. Conceitos e Princípios
   2. Vulnerabilidades x Prevenção
   3. Redes Sociais
   4. Criptografia
   5. Jogo on-line criptografia
5. Unidade 2 - Programas Maliciosos - Malware
   1. Vírus
   2. Bot e Botnet
   3. Spyware
   4. Backdoor
   5. Cavalo de Tróia
   6. Ransomware
   7. Desafio Prático
   8. Tutorial Desafio Prático
   9. Estudo de caso - Malware
   10. Videoconferência
6. Unidade 3 - Golpes e ataques na Internet
   1. Varredura em redes (Scan)
   2. Falsificação de e-mail (E-mail spoofing)
   3. Spam
   4. Furto de identidade
   5. Fraude de antecipação de recursos (Advance fee fraud)
   6. Phishing
   7. Golpes de comércio eletrônico
   8. Interceptação de tráfego (Sniffing)
   9. Força bruta (Brute force)
   10. Desfiguração de página (Defacement)
   11. Negação de serviço (DoS e DDoS)
   12. Desafio Prático
   13. Tutorial desafio prático
   14. Videoconferência
   15. Estudo de caso - Golpe comércio eletrônico
7. Prova Final (pós teste)
8. Avaliação de satisfação com o curso

**PRÉ E PÓS TESTE**

1. - Qual o seu nome?
2. - Qual ano você cursa? ( ) 1º ( ) 2º ( ) 3º ( ) 4º
3. - Qual seu telefone (Preferencialmente Zap)?
4. - Considerando seus conhecimentos sobre segurança da informação e o texto a seguir: “É uma falha ou fraqueza de procedimento, design, implementação, ou controles internos de um sistema que possa ser acidentalmente ou propositalmente explorada, resultando em uma brecha de segurança ou violação da política de segurança do sistema”. Essa definição de se refere a:
   1. Risco
   2. Fragilidade
   3. Ameaça
   4. Impacto
   5. Vulnerabilidade
5. - A figura acima apresenta um cenário no qual uma pessoa usa uma vara e uma corda C para atravessar o ponto 1 para o ponto 2, na presença de A e B. Com base na figura e nos seus conceitos sobre segurança da informação, julgue os itens subsequentes**.**
   1. A representante uma vulnerabilidade
   2. A representante uma ameaça
   3. A representante um risco
   4. A representante um impacto
   5. A representa um ativo
6. - A figura abaixo apresenta um cenário no qual uma pessoa usa uma vara e uma corda C para atravessar o ponto 1 para o ponto 2, na presença de A e B. Com base na figura e nos seus conceitos sobre segurança da informação, julgue os itens subsequentes.
   1. C representa uma ameaça
   2. C representa um risco
   3. C representa uma vulnerabilidade
   4. C representa um ataque
   5. C representa um ativo
7. - A Segurança da Informação (SI) é especializada na proteção de um conjunto de informações com fim de preservação ou valor que possui para um indivíduo ou organização. Sobre como propriedades básicas de segurança da informação, marque uma alternativa correta.

( ) Disponibilidade, rastreabilidade e simplicidade ( ) Rastreabilidade, usabilidade e notoriedade

( ) Confidencialidade, integridade e disponibilidade ( ) Integridade, usabilidade e simplicidade

( ) Confidencialidade, autenticação e disponibilidade

1. - Um Técnico de Informática está analisando como recursos de diversas pragas virtuais (malwares), para executar a instalação do antivírus adequado. Dentre as características específicas por ele analisadas, estão:

I. Programa que, além de executar as funções para as quais foram executadas, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário. Um exemplo é um programa que recebe ou obtém sites na Internet e que parece ser inofensivo. Esse programa geralmente consiste em um único arquivo e é explicitamente executado para que seja instalado no computador. II.

Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído na ação de outros códigos maliciosos, que podem afetar o computador ou atacantes que exploram vulnerabilidades existentes nos programas utilizados no computador. Após incluído, ele é usado para garantir o acesso futuro ao computador comprometido, permitir que ele seja acessado remotamente, caso haja necessidade de executar novamente os métodos de execução de invasão ou infecção e, na maioria dos casos, sem que seja notado. III. Programa que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia. O atacante exige pagamento de resgate para restabelecer o acesso ao usuário. As descrições acima são, corretas e respectivamente, correspondentes a:

( ) Cavalo de Troia (trojan), backdoor e Ransomware ( ) Worm, backdoor e vírus

( ) Vírus, spyware e rootkit

( )Spyware, cavalo de Troia (trojan) e Ransomware ( )Bot, Rootkit e cavalo de Tróia (Trojan)

1. - Existem diversos tipos de códigos maliciosos, entre eles o spyware. Acerca desse assunto, é correto afirmar que Spyware consiste em:

( ) Programa ou parte de um programa de computador, normalmente malicioso, que se propaga, inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos.

( ) Programa que além de projetar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, sem o conhecimento do usuário.

( ) Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para esse fim.

( ) Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

( ) Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

1. - O é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. É notadamente responsável por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costuma propagar e, como consequência, pode afetar o desempenho da rede e a utilização do computador. Assinale a alternativa que CORRETAMENTE preenche a lacuna do texto acima.

( ) Vírus ( ) Trojan

( )Spyware

( )Keylogger ( ) Worm

1. - E-mail spoofing é uma técnica que pode ser utilizada para propagação de códigos maliciosos, envio de spam e golpes de phishing. Esta técnica consiste em:

( ) Alterar as configurações de um servidor de e-mail para que dispare uma infinidade de e-mails falsos até encher a caixa de correio de um ou muitos usuários

( ) Falsificar o protocolo SMTP para inspecionar os dados trafegados na caixa de e- mail do usuário, por meio do uso de programas específicos.

( ) Alterar os campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

( ) Efetuar buscas minuciosas no computador do usuário, com o objetivo de identificar informações sigilosas.

( ) Alterar os campos do protocolo SMTP, de forma que os e-mails do usuário sejam direcionados para outra sem que ele saiba.

1. - Das alternativas a seguir, assinale a única que contém eventos que caracterizam uma tentativa de ataque do tipo força bruta.

( ) Brechas resultantes de bugs no sistema

( ) Sobrecarga de servidores, alcançada por meio de ataques simultâneos e descentralizados

( ) A operação local e não autorizada de estações ou servidores

( ) A repetição automática de tentativas de acesso a um recurso protegido, com senhas criadas a partir de combinações aleatórias ou extraídas de listas pré-definidas.

( ) A captura de dados sensíveis a partir de um programa espião instalado no computador do usuário.

1. - A técnica de Sniffing

( ) Utiliza um ou mais computadores para tornar indisponível um serviço provido ( ) Tenta adivinhar por tentativa e erro a senha de um usuário.

( ) Captura e inspeciona dados que trafegam em uma rede

( ) Altera campos do cabeçalho de mensagens de e-mail para falsificar a origem da mensagem

( ) Altera o conteúdo de páginas web de forma maliciosa e publica informações contra a instituição mantenedora da página web.

1. - Spam e Spyware são basicamente:

( ) Dois softwares do typo player de vídeo

( ) Dois tipos de vírus fatais que podem danificar um computador.

( ) Respectivamente, um e-mail não solicitado e um programa espião ( ) Respectivamente, um programa espião e um e-mail não solicitado ( ) Respectivamente, um e-mail espião e um vírus de computador.

1. - Vários computadores de uma rede estão gerando spam, disseminando vírus, atacando computadores e servidores de forma não prevista pelos administradores. Foi identificado um malware que é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados nos computadores infectados, tornando-os zumbis. Tal comportamento é tipicamente ocasionado por uma ação de

( )Keylogger ( )Botnet

( ) Adware ( )Phishing ( )Spyware

1. - Na quinta-feira de manhã, John, um empregado da universidade XYZ, notou uma mensagem de aviso em seu computador dizendo que o sistema foi atacado por um Win32.VB worm. Mesmo que o software antivírus estava presente no sistema, o software não conseguiu detectar o novo worm porque não foi atualizado para a versão mais recente. Quando John tentou abrir seu e-mail, ele experimentou uma conexão de internet lenta. Ele percebeu que havia alguns nomes de arquivo incomuns no disco. John imediatamente informou seu amigo Bob, que também era um empregado XYZ, do problema. Bob checou seu computador em seu escritório e experimentou o mesmo problema que John. John e Bob verificado vários computadores nos laboratórios, e descobriu que Win32.VB verme havia infectado muitos outros computadores no laboratório. Eles contataram o setor de TI da Universidade XYZ. O administrador do sistema verificou os computadores constatando o incidente de segurança da informação. Como um resultado do ataque verme as atividades no laboratório da

Universidade XYZ foram suspensas, o que causou um grande inconveniente. Na sua opinião, qual foi a vulnerabilidade explorada? Quais medidas devem ser adotadas para conter e se recuperar do incidente de segurança da informação relatado no estudo de caso acima?

1. - Você está acessando uma rede social logado em sua conta pessoal e de repente visualiza um anúncio do site americanas contendo uma promoção imperdível de máquina de lavar. Como tinha feito recentemente uma pesquisa, comparando preços e marcas desse produto, percebe que o valor do anúncio se encontra muito abaixo do praticado no mercado. Ao clicar é redirecionado para uma página muito semelhante a da americanas, que detalha melhor a promoção, explica que você deve aproveitar a oportunidade relâmpago, que é possível comprar com apenas um clique (não é necessário cadastro) e afirma que a única modalidade de pagamento é por meio de boleto bancário. Sendo assim, salienta que a promoção está acabando naquele mesmo dia e que restam apenas poucas unidades do produto em estoque. Após gerar o boleto bancário e efetuar o pagamento da compra você tenta acompanhar o envio do produto pelo número do pedido descrito no boleto. Porém, não consegue visualizar o pedido cadastrado para sua compra no site, entra em contato telefônico pelo canal de atendimento ao cliente e percebe que foi vítima de um golpe. De acordo com os conhecimentos adquiridos no curso identifique quais vulnerabilidades podem ter sido exploradas para enganar o usuário? Identifique quais estratégias de golpe foram utilizadas? Explique quais ações o usuário deveria ter adotado para identificar a fralde? O que deve ser feito caso o usuário efetue o pagamento do boleto fraudulento?
2. - Crie um arquivo de "vírus" com o nome "DOCUMENTO" que seja capaz de desligar a máquina do usuário quando ele executar o arquivo.
3. - Considerando as estratégias de golpe e ataques que ocorrem na internet, faça a cópia de uma página que contenha uma oferta real em um site de vendas conhecido como: magazine Luíza, Americanas, Ricardo eletro ou outro...

X

#### [Curso em Segurança da Informação](https://mooc-seginfo.appspot.com/moocseg/)

[williamdasilvamelo@gmail.com](mailto:williamdasilvamelo@gmail.com) | [Dashboard](https://mooc-seginfo.appspot.com/moocseg/dashboard) | Sair

[Notificações](https://mooc-seginfo.appspot.com/moocseg/announcements) [**Curso**](https://mooc-seginfo.appspot.com/moocseg/course)[Progresso](https://mooc-seginfo.appspot.com/moocseg/student/home)

[Curso](https://mooc-seginfo.appspot.com/moocseg/course) › [Unidade 1](https://mooc-seginfo.appspot.com/moocseg/unit?unit=16)

**Search**

## Unidade 1 - Introdução [](https://mooc-seginfo.appspot.com/moocseg/dashboard?action=edit_unit&amp;key=16)

 [1.1 Conceitos e Princípios](https://mooc-seginfo.appspot.com/moocseg/unit?unit=16&amp;lesson_title_18)



 [1.2](https://mooc-seginfo.appspot.com/moocseg/unit?unit=16&amp;lesson_title_17)

[Vulnerabilidades x Prevenção](https://mooc-seginfo.appspot.com/moocseg/unit?unit=16&amp;lesson_title_17)

 [1.3 Redes sociais](https://mooc-seginfo.appspot.com/moocseg/unit?unit=16&amp;lesson_title_34)

 [1.4 Criptografia](https://mooc-seginfo.appspot.com/moocseg/unit?unit=16&amp;lesson_title_35)

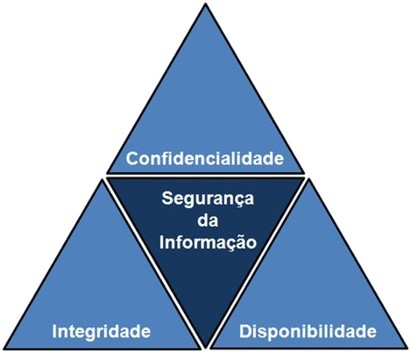
Conceitos e Princípios 

Devido à tamanha importância da informação, a necessidade de protegê-las passou a ser crucial. Quando falamos em segurança da informação, estamos nos referindo a tomar ações para garantir a confidencialidade, integridade, disponibilidade e demais aspectos da segurança das informações.

Vejamos os conceitos destes três principais pilares:

**Confidencialidade**: “Garantia de que o acesso à informação é restrito aos seus usuários legítimos.” (Beal, 2008, p. 1). Ou seja, seu acesso é permitido apenas a determinados usuários.

**Integridade**: “Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais” (Sêmola, 2003, p. 45). Ou seja, informação não adulterada.

**Disponibilidade**: “Garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna” (Beal, 2008, p. 1). Ou seja, independente da finalidade, a informação deve estar disponível.

Além destes, segundo Lyra (2008, p.4), podemos citar mais alguns aspectos complementares para garantia da segurança da informação:

**Autenticidade**: “Garantir que um usuário que esta enviando ou manipulando a informação é de fato quem alega ser”

**Não repúdio**: “Capacidade do sistema de provar que um usuário executou uma determinada ação”. Lyra (2008, p.4)

**Legalidade**: “Garantir que o sistema esteja aderente à legislação”.

**Privacidade**: “Capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações”.

**Auditoria**: “Capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque”.

**Vulnerabilidade**

A vulnerabilidade está intimamente ligada ao ponto fraco de um ativo, ou seja, pode ser entendida como uma fragilidade. Trata-se de um erro no procedimento (no caso de sistemas), falha de um agente ou má configuração dos aplicativos de segurança, de maneira não proposital ou proposital, gerando assim, uma informação não confiável. Quando isso ocorre, temos um “rompimento” de um ou mais princípios da segurança da informação.

Beal (2008, p. 14) elucida o conceito de vulnerabilidade como sendo uma “fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque”.

Em complemento a este conceito, Lyra (2008, p.06) afirma que:

Essas vulnerabilidades poderão ser exploradas ou não, sendo possível que um ativo da informação apresente um ponto fraco que nunca será efetivamente explorado. Após serem detectadas falhas é necessário tomar algumas providências. O primeiro passo é identificar a falha, onde esta aconteceu e tentar corrigi-la da melhor maneira.

**Ameaça**

Ameaça pode ser considerada como um possível evento ou atitude indesejável que potencialmente remove, desabilita ou destrói um recurso. As ameaças normalmente aproveitam das falhas de segurança da organização, a possibilidade de um agente (ou fonte de ameaça) explorar acidentalmente ou propositalmente uma vulnerabilidade especifica.

Os agentes podem ser pessoas, eventos, meio ambiente, sistemas, etc. Exemplos de

ameaças acidentais são falhas de hardware, desastres naturais, erros de programação, etc; enquanto que ameaças propositais podem entendidas por roubos, invasões, fraudes, dentre outros. Assim, dizemos que determinada situação é geradora de uma ameaça se o seu agente tiver possibilidades ou capacidades para a sua concretização

**Risco**

Um risco de segurança é um evento possível e potencialmente danoso a uma organização, isto é, um evento hipotético, que possui chance de ocorrência futura que não é nula e que apresenta impacto negativo significante.

Sem chance de ocorrência futura, um evento hipotético não se configura como risco. Sem impacto negativo significante, um evento hipotético não se configura como risco. Assim, risco de segurança da informação é o “Potencial que uma ameaça explore vulnerabilidades de um ativo ou conjunto de ativos e desta forma prejudique uma organização. Um risco é mensurado em termos de probabilidade de materialização do risco e seus impactos.

**Riscos x Ameaças x Vulnerabilidades**

Risco de segurança é uma combinação de ameaças, vulnerabilidades e impactos. Ameaças são eventos que exploram vulnerabilidades (fragilidades) e podem causar danos. Logo, risco é tudo aquilo que pode acontecer em um momento futuro, associado ao seu impacto potencial. O risco pode ser interpretado como um evento que se efetivamente vier a acontecer, causará um impacto. Nesse sentido, o evento só se evidencia quando nós temos um agente (ameaça) e uma vulnerabilidade (fraqueza).

Utilizando o exemplo do celular, você deixou o celular desbloqueado e sem senha em cima da mesa de um barzinho e foi ao banheiro, a ameaça é um ladrão pegar seu celular, a vulnerabilidade é estar desbloqueado e sem senha. Com isso, você sofre o risco de suas informações contidas no celular serem compartilhadas.

**Nesse sentido, percebemos que o risco está intimamente ligado ao impacto (dano real), a ameaça está muito mais relacionada com os agentes e as vulnerabilidades são as fraquezas que podem ser exploradas..**

**Ataque**

Conhecidos os conceitos de Vulnerabilidade e Ameaça, torna-se fácil compreender o que seria um ataque. Segundo Beal (2008, p.14), trata-se de um “evento decorrente da exploração de uma vulnerabilidade por uma ameaça”, em outras palavras um ataque representa a concretização de uma ameaça.

Segundo Dias (2000, p.77), os ataques podem ser categorizados em passivos e ativos:

**Passivos**: São aqueles que não interferem no conteúdo do recurso que foi atacado, como por exemplo, observação e conhecimento de informações armazenadas nos

sistemas institucionais ou análise de tráfego de uma rede.

**Ativos**: Prejudicam diretamente o conteúdo do recurso atacado, modificando e eliminando informações ou gerando informações falsas.

**Engenharia social**

Técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto desse curso, é considerada uma prática de má-fé, usada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O popularmente conhecido "conto do vigário" utiliza engenharia social.

Na maioria dos casos, os engenheiros sociais bem-sucedidos têm uma habilidade muito boa em lidar com as pessoas. Eles são charmosos, educados e agradam facilmente — os traços sociais necessários para estabelecer a afinidade e confiança. Assim como uma marionete é manipulada pelo homem, a vítima de uma extorsão também é, para isso basta que o farsante adquira a confiança do indivíduo, através de um mínimo conhecimento que se tenha da empresa e assim alcançar a informação desejada.

As técnicas mais costumeiras, que podem ser usadas de maneira individual ou combinadas, são:

**Contatos telefônicos**, simulando atendimento de suporte ou uma ação de emergência;

**Contato através de e-mail**, atuando como estudante com interesse em pesquisa sobre determinado assunto ou como pessoa com interesse específico em assunto de conhecimento da vítima;

**Obtenção de informações vazadas** em listas de discussão ou comunidades virtuais na Internet;

**Varredura do lixo informático**, para obtenção de informações adicionais para tentativas posteriores de contato;

**Disfarce de equipe de manutenção**; o atacante usa um disfarce para ter acesso a locais restritos, age como fosse prestar algum serviço, mas na verdade ele vai utilizar métodos para alcançar seu real objetivo: Obter dados confidenciais.

**Visita em pessoa, como estudante**, estagiário ou pessoa com disfarce de ingenuidade.

Um dos casos mais emblemáticos de engenharia social é a eleição presidencial dos Estados Unidos em 2016. Ataques de spear phishing levaram ao vazamento de e-mails e informações do Partido Democrata que podem ter influenciado o resultado da eleição, com a vitória de Donald Trump sobre Hillary Clinton. Os hackers criaram um e-mail falso no Gmail, convidando os usuários, por meio de um link, a alterar as suas senhas devido a atividades incomuns. Os

fraudadores então tiveram acesso a centenas de e-mails contendo informações confidenciais sobre a campanha de Clinton.

[Confidencialidade - Segurança da I…](https://www.youtube.com/watch?v=HMpt0DqYa9c)

[Disponibilidade - Segurança da Info…](https://www.youtube.com/watch?v=ydj04k2Wc7Y)

[…](https://www.youtube.com/watch?v=chBAQxW701U)

[Integridade - Segurança da Informa](https://www.youtube.com/watch?v=chBAQxW701U)

A Segurança da Informação (SI) é especializada na proteção de *Um ponto* um conjunto de informações com fim de preservação ou valor que possui para um indivíduo ou organização. Quais são os três pilares básicos de segurança da informação, escolha abaixo a alternativa correta.

Confidencialidade, integridade e disponibilidade Rastreabilidade, usabilidade e notoreidade Disponibilidade, rastreabilidade e simplicidade Integridade, usabilidade e simplicidade Confidencialidade, autenticação e disponibilidade

**Referências**



**Conferir resposta**

BEAL, Adriana. **Segurança da Informação**. Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações. São Paulo. Atlas, 2005 – Reimpressão 2008.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. Axcel Books. Rio de Janeiro, 2000.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**. Uma visão executiva. Rio de Janeiro. Elsevier, 2003 – 11º reimpressão.

LYRA, Maurício Rocha. **Segurança e Auditoria em Sistemas de Informação** Rio de Janeiro. Ciência Moderna, 2008.



**Vulnerabilidades x Prevenção** 



Nesse ponto, já compreendemos que a **vulnerabilidade** consiste em qualquer fraqueza que possa comprometer a segurança de sistemas ou informações. Ou seja, fragilidade que pode ser explorada por uma ou mais ameaças. Sendo assim, chama a atenção para algumas das vulnerabilidades bem comuns:

Versões e patches de segurança de programas desatualizados;

Utilização de programas piratas

Inexistência de mecanismo de proteção (antivírus)

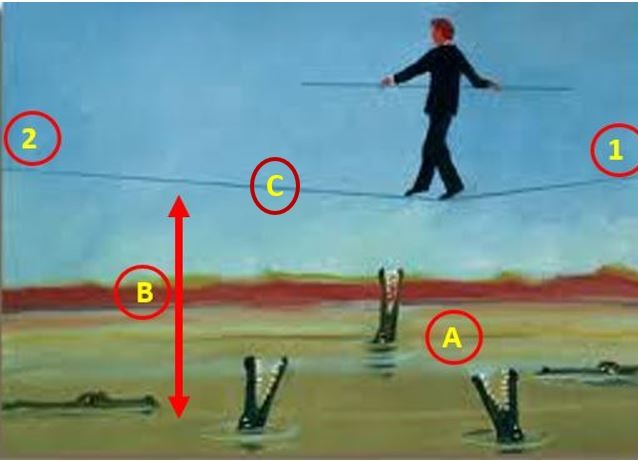
Mecanismo de proteção desatualizado

Essas vulnerabilidades listadas acima podem parecer simples de serem resolvidas e realmente são. Entretanto, os impactos que podem causar casos não resolvidos podem ser bem graves.

Na sexta-feira, 12 de maio de 2017, uma série de ataques em escala global usando uma versão usada para criptografar-ransomware WanaCrypt0r. Nessa versão, uma novidade: um ransomware com funções de worm, o primeiro ransomworm da história!

Uma série de ataques em escala global, usando uma versão afetada de ransomware de criptografia, ou o WanaCrypt0r 2.0 afeta como áreas públicas e públicas ao redor do mundo, passando de 150 países e 350 mil máquinas infectadas. Até a NSA - Agência Nacional de Segurança, dos EUA, sofreu com esse incidente.

Isso ocorre porque tudo começou com uma vulnerabilidade no sistema operacional da Microsoft, ou Windows. Essa vulnerabilidade foi exposta pelo grupo Os Shadow Brokers, uma Microsoft, no entanto, já criaram o patch de correção no mês anterior, em março. Ou seja, os terminais afetados pelo ataque global de ransomware estavam com seus sistemas operacionais Windows desatualizados. Assim, uma das boas práticas de segurança segura é uma garantia de que o ambiente está com todas as suas aplicações atuais e seguras.



A figura acima apresenta um cenário no qual uma pessoa usa *Um ponto* uma vara e uma corda C para atravessar o ponto 1 para o ponto 2, na presença de A e B. Com base na figura e nos conceitos de segurança da informação, julgue os itens subsequentes.

A representante uma vulnerabilidade A representante um risco

A representa um ativo

A representante um impacto A representante uma ameaça

A figura acima apresenta um cenário no qual uma pessoa usa *Um ponto*

**Conferir resposta**

uma vara e uma corda C para atravessar o ponto 1 para o ponto 2, na presença de A e B.Com base na figura e nos conceitos de segurança da informação, julgue os itens subsequentes.

C representa um ataque C representa um ativo

C representa uma ameaça

C representa uma vulnerabilidade



C representa um risco

**Conferir resposta**

**Prevenção**



Agora, se você já está usando alguns dos riscos relacionados ao uso de Tecnologias Digitais de Informação e Comunicação, o TDIC e que, apesar disso, reconhece que não é possível deixar de usar esses recursos, não está no momento de aprender detalhadamente a se proteger.

Para permitir que você possa utilizar com segurança como tecnologias digitais de informação e comunicação (TDIC), é necessário que os serviços disponibilizados e as notificações sejam auditadas por este meio garantido alguns requisitos básicos de segurança, como:

**Identificação:** permitir que uma entidade se identifique, ou seja, diga quem ela é.

**Autenticação:** verifique se a entidade é realmente quem ela diz ser.

**Autorização:** determine como ações que podem ser executadas.

**Integridade:** proteger uma informação contra alteração não autorizada.

**Confidencialidade ou sigilo:** proteger uma informação contra acesso não autorizado.

**Não repúdio:** evitar que uma entidade possa negar que foi ela quem executou uma ação.

**Disponibilidade:** garantir que um recurso esteja disponível sempre que necessário.

Para testar e garantir esses requisitos, os adaptadores e os ativos dos mecanismos de segurança, quando configurados e usados corretamente, podem ajudar a proteger os riscos causados pelo uso da tecnologia.

**Recomendações**

**Mantenha os programas instalados com as versões mais recentes:**

Os fabricantes costumam lançar novas versões quando há recursos usados e vulnerabilidades que são corrigidas. Sempre que uma nova versão para lançada, ela deve ser automaticamente ativada, isso pode ajudar a proteger seu computador de ações e códigos maliciosos. Além disso, alguns fabricantes usam o suporte e desenvolvem aplicativos para testes antigos, o que significa que as vulnerabilidades podem vir a ser descobertas não corrigidas.

**Mantenha os programas instalados com todas as atualizações aplicadas:**

Quando vulnerabilidades são descobertas, certos fabricantes costumam alterar alterações específicas, chamadas de patches, hot fixes ou service packs. Portanto, para manter os programas livres de vulnerabilidades, além de manter as versões mais recentes, é importante que sejam aplicadas todas as atualizações disponíveis. configurar, quando possível, para que programas sejam selecionados automaticamente;

**Use apenas alguns programas originais:**

O uso de programas não originais pode colocar em risco a segurança do seu computador, já que muitos fabricantes não podem obter atualizações quando detectados não licenciados. Além disso, uma instalação de programas deste tipo, uma exibição de mídias e sites não reproduzidos ou através de programas de compartilhamento de arquivos, pode incluir uma instalação de códigos maliciosos.

**Use mecanismos de proteção:**

O uso de mecanismos de proteção, como programas antimalware e firewall pessoal, pode contribuir para o seu computador que não seja infectado / invadido e que não participe de atividades maliciosas.

As ferramentas antimalware são aquelas que podem detectar e remover códigos maliciosos de um computador. Antivírus, antispyware, antirootkit e antitrojan são exemplos de ferramentas deste tipo.

Entre as diferentes ferramentas existentes, que aumentam a maior quantidade de funcionalidades ou antivírus. Embora tenham sido criados para interpretar sobre vírus, ou para passar o tempo, também são incluídos como recursos de outros programas, fazendo com que alguns deles caiam em desuso

**Existem diversos tipos de programas antimalware que diferem entre as seguintes formas:**

**Método de detecção** : assinatura (uma lista de assinaturas é usado à procura de padrões), heurística (baseia-se nas estruturas, instruções e recursos que o código malicioso possui) e comportamento (baseia-se no comportamento do código malicioso quando executado), alguns dos métodos mais comuns.

**Forma de uso** : pode ser gratuito (quando disponível gratuitamente na Internet e usado por prazo indeterminado), experimentos (avaliação, usados livremente por um período predeterminado) e pagos (solicitados que uma licença seja usada). Um mesmo fabricante pode disponibilizar mais um tipo de programa, sendo que a versão gratuita usa os recursos básicos ao passo que a versão paga possui recursos extras, além de poder contar com suporte.

**Execução** : pode ser instalado localmente no computador ou executar sob demanda por intermédio do navegador Web. Também podem ser online, quando enviados para serem executados em servidores remotos, por um ou mais programas.

**Funcionalidades incluídas:**

O lém das funções básicas (detectar, remover e remover códigos maliciosos) também pode apresentar outras funcionalidades integradas, como a possibilidade de geração de discos de emergência e firewall pessoal.

**Mais Recomendações**

utilizar programas online quando suspeitar que o antimalware local esteja desativado / comprometido ou quando for necessária uma segunda opinião (escolha confirmar ou estado de um arquivo que já foi verificado pelo antimalware local)

configurar o antimalware para verificar toda e qualquer extensão de arquivo;

configurar o antimalware para verificar automaticamente arquivos anexados a e-mails e acessados pela Internet;

configurar o antimalware para verificar automaticamente os discos rígidos e as unidades removíveis (como pen-drives, CDs, DVDs e discos externos);

mantenha o arquivo de assinaturas sempre atualizado (configure o antimalware para atualizá-lo automaticamente pela rede, de preferência diária);

mantenha o antimalware sempre atualizado, com uma versão mais recente e com todas as atualizações aplicadas;

evitar executar diferentes programas antimalware (eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção de outro);

crie um disco de emergência e utilize-o quando o antimalware estiver desconectado / comprometido ou o comportamento do computador para estranho (mais lento, gravando ou lendo ou disco rígido com muita frequência, etc.).

[Defenda-se dos Vírus de Computa…](https://www.youtube.com/watch?v=PM7alPg_6Kw)

Redes sociais 



As redes sociais permitem que os usuários criem perfis e os utilizem para se conectar a outros usuários, compartilhar informações e se agrupar de acordo com interesses em comum. Alguns exemplos são: Facebook, Instagram, Twitter, Linkedin, Google+ e foursquare.

As redes sociais, atualmente, já fazem parte do cotidiano de grande parte do usuários da Internet, que as utilizam para se informar sobre os assuntos do momento e para saber o que seus amigos e ídolos estão fazendo, o que estão pensando e onde estão. Também são usadas para outros fins, como seleção de candidatos para vagas de emprego, pesquisas de opinião e mobilizações sociais.

As redes sociais possuem algumas características próprias que as diferenciam de outros meios de comunicação, como a velocidade com que as informações se propagam, a grande quantidade de pessoas que elas conseguem atingir e a riqueza de informações pessoais que elas disponibilizam. Essas características, somadas ao

alto grau de confiança que os usuários costumam depositar entre si, fez com que as redes sociais chamassem a atenção, também, de pessoas mal-intencionadas.

**Alguns dos principais riscos relacionados ao uso de redes sociais são:**

**Contato com pessoas mal-intencionadas**: qualquer pessoa pode criar um perfil falso, tentando se passar por uma pessoa conhecida e, sem que saiba, você pode ter na sua rede (lista) de contatos pessoas com as quais jamais se relacionaria no dia a dia.

**Furto de identidade**: assim como você pode ter um impostor na sua lista de contatos, também pode acontecer de alguém tentar se passar por você e criar um perfil falso. Quanto mais informações você divulga, mais convincente o seu perfil falso poderá ser e maiores serão as chances de seus amigos acreditarem que estão realmente se relacionando com você.

**Invasão de perfil**: por meio de ataques de força bruta, do acesso a páginas falsas ou do uso de computadores infectados, você pode ter o seu perfil invadido. Atacantes costumam fazer isto para, além de furtar a sua identidade, explorar a confiança que a sua rede de contatos deposita em você e usá-la para o envio de spam e códigos maliciosos.

**Uso indevido de informações**: as informações que você divulga, além de poderem ser usadas para a criação de perfil falso, também podem ser usadas em ataques de força bruta, em golpes de engenharia social e para responder questões de segurança usadas para recuperação de senhas.

**Invasão de privacidade**: quanto maior a sua rede de contatos, maior é o número de pessoas que possui acesso ao que você divulga, e menores são as garantias de que suas informações não serão repassadas. Além disso, não há como controlar o que os outros divulgam sobre você.

**Vazamento de informações**: há diversos casos de empresas que tiveram o conteúdo de reuniões e detalhes técnicos de novos produtos divulgados na Internet e que, por isto, foram obrigadas a rever políticas e antecipar, adiar ou cancelar decisões.

**Disponibilização de informações confidenciais**: em uma troca "amigável" de mensagens você pode ser persuadido a fornecer seu e-mail, telefone, endereço, senhas, número do cartão de crédito, etc. As consequências podem ser desde o recebimento de mensagens indesejáveis até a utilização do número de seu cartão de crédito para fazer compras em seu nome.

**Recebimento de mensagens maliciosas**: alguém pode lhe enviar um arquivo contendo códigos maliciosos ou induzi-lo a clicar em um link que o levará a uma página Web comprometida.

**Acesso a conteúdos impróprios ou ofensivos**: como não há um controle imediato sobre o que as pessoas divulgam, pode ocorrer de você se deparar com mensagens ou imagens que contenham pornografia, violência ou que incitem o ódio e o racismo.

**Danos à imagem e à reputação**: calúnia e difamação podem rapidamente se propagar, jamais serem excluídas e causarem grandes danos às pessoas envolvidas, colocando em risco a vida profissional e trazendo problemas familiares, psicológicos e

de convívio social. Também podem fazer com que empresas percam clientes e tenham prejuízos financeiros.

**Sequestro**: dados de localização podem ser usados por criminosos para descobrir a sua rotina e planejar o melhor horário e local para abordá-lo. Por exemplo: se você fizer check-in (se registrar no sistema) ao chegar em um cinema, um sequestrador pode deduzir que você ficará por lá cerca de 2 horas (duração média de um filme) e terá este tempo para se deslocar e programar o sequestro.

**Furto de bens**: quando você divulga que estará ausente por um determinado período de tempo para curtir as suas merecidas férias, esta informação pode ser usada por ladrões para saber quando e por quanto tempo a sua residência ficará vazia. Ao retornar, você pode ter a infeliz surpresa de descobrir que seus bens foram furtados.

A seguir, observe alguns cuidados que você deve ter ao usar as redes sociais.

**Preserve a sua privacidade:**

considere que você está em um local público, que tudo que você divulga pode ser lido ou acessado por qualquer pessoa, tanto agora como futuramente;

pense bem antes de divulgar algo, pois não há possibilidade de arrependimento. Uma frase ou imagem fora de contexto pode ser mal-interpretada e

causar mal-entendidos. Após uma informação ou imagem se propagar, dificilmente ela poderá ser totalmente excluída;

use as opções de privacidade oferecidas pelos sites e procure ser o mais restritivo possível (algumas opções costumam vir, por padrão, configuradas como públicas e devem ser alteradas);

mantenha seu perfil e seus dados privados, permitindo o acesso somente a pessoas ou grupos específicos;

procure restringir quem pode ter acesso ao seu endereço de e-mail, pois muitos spammers utilizam esses dados para alimentar listas de envio de spam;

seja seletivo ao aceitar seus contatos, pois quanto maior for a sua rede, maior será o número de pessoas com acesso às suas informações. Aceite convites de pessoas que você realmente conheça e para quem contaria as informações que costuma divulgar;

não acredite em tudo que você lê. Nunca repasse mensagens que possam gerar pânico ou afetar outras pessoas, sem antes verificar a veracidade da informação;

seja cuidadoso ao se associar a comunidades e grupos, pois por meio deles muitas vezes é possível deduzir informações pessoais, como hábitos, rotina e classe social.

**Seja cuidadoso ao fornecer a sua localização:**

observe o fundo de imagens (como fotos e vídeos), pois podem indicar a sua localização;

não divulgue planos de viagens e nem por quanto tempo ficará ausente da sua residência;

ao usar redes sociais baseadas em geolocalização, procure se registrar (fazer check-in) em locais movimentados e nunca em locais considerados perigosos; ao usar redes sociais baseadas em geolocalização, procure fazer check-in quando sair do local, ao invés de quando chegar.

**Respeite a privacidade alheia:**

não divulgue, sem autorização, imagens em que outras pessoas apareçam;

não divulgue mensagens ou imagens copiadas do perfil de pessoas que restrinjam o acesso;

seja cuidadoso ao falar sobre as ações, hábitos e rotina de outras pessoas; tente imaginar como a outra pessoa se sentiria ao saber que aquilo está se tornando público.

Previna-se contra códigos maliciosos e phishing:

mantenha o seu computador seguro, com os programas atualizados e com todas as atualizações aplicadas;

utilize e mantenha atualizados mecanismos de proteção, como antimalware e firewall pessoal;

desconfie de mensagens recebidas mesmo que tenham vindo de pessoas conhecidas, pois elas podem ter sido enviadas de perfis falsos ou invadidos; seja cuidadoso ao acessar links reduzidos. Há sites e complementos para o seu navegador que permitem que você expanda o link antes de clicar sobre ele.

**Proteja o seu perfil:**

seja cuidadoso ao usar e ao elaborar as suas senhas;

habilite, quando disponível, as notificações de login, pois assim fica mais fácil perceber se outras pessoas estiverem utilizando indevidamente o seu perfil;

use sempre a opção de logout para não esquecer a sessão aberta;

denuncie casos de abusos, como imagens indevidas e perfis falsos ou invadidos.

**Proteja sua vida profissional:**

cuide da sua imagem profissional. Antes de divulgar uma informação, procure avaliar se, de alguma forma, ela pode atrapalhar um processo seletivo que você venha a participar (muitas empresas consultam as redes sociais à procura de informações sobre os candidatos, antes de contratá-los);

verifique se sua empresa possui um código de conduta e procure estar ciente dele. Observe principalmente as regras relacionadas ao uso de recursos e divulgação de informações;

evite divulgar detalhes sobre o seu trabalho, pois isto pode beneficiar empresas concorrentes e colocar em risco o seu emprego;

preserve a imagem da sua empresa. Antes de divulgar uma informação, procure avaliar se, de alguma forma, ela pode prejudicar a imagem e os negócios da empresa e, indiretamente, você mesmo;

proteja seu emprego. Sua rede de contatos pode conter pessoas do círculo profissional que podem não gostar de saber que, por exemplo, a causa do seu cansaço ou da sua ausência é aquela festa que você foi e sobre a qual publicou diversas fotos;

use redes sociais ou círculos distintos para fins específicos. Você pode usar, por exemplo, uma rede social para amigos e outra para assuntos profissionais ou separar seus contatos em diferentes grupos, de forma a tentar restringir as informações de acordo com os diferentes tipos de pessoas com os quais você se relaciona;

**Proteja seus filhos:**

procure deixar seus filhos conscientes dos riscos envolvidos no uso das redes sociais;

procure respeitar os limites de idade estipulados pelos sites (eles não foram definidos à toa);

oriente seus filhos para não se relacionarem com estranhos e para nunca fornecerem informações pessoais, sobre eles próprios ou sobre outros membros da família;

oriente seus filhos a não divulgarem informações sobre hábitos familiares e nem de localização (atual ou futura);

oriente seus filhos para jamais marcarem encontros com pessoas estranhas; oriente seus filhos sobre os riscos de uso da webcam e que eles nunca devem utilizá-la para se comunicar com estranhos;

procure deixar o computador usado pelos seus filhos em um local público da casa (dessa forma, mesmo a distância, é possível observar o que eles estão fazendo e verificar o comportamento deles).

[Você tem vida privada de verdade (…](https://www.youtube.com/watch?v=GSI7tf-Z9S0)



**Criptografia** 

A criptografia, considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, é um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso da Internet.

A primeira vista ela até pode parecer complicada, mas para usufruir dos benefícios que proporciona você não precisa estudá-la profundamente e nem ser nenhum matemático experiente. Atualmente, a criptografia já está integrada ou pode ser facilmente adicionada à grande maioria dos sistemas operacionais e aplicativos e



Considere o texto a seguir: “Uma falha ou fraude no*Um ponto* procedimento, design, implementação, ou controles internos de um sistema que podem ser acidentalmente ou propositalmente explorados, resultando em uma violação de segurança ou violação da política de segurança do sistema”. No contexto de segurança da informação, essa é uma definição de:

Risco Impacto Ameaça

Vulnerabilidade Engenharia social

**Conferir resposta**

para usá-la, muitas vezes, basta a realização de algumas configurações ou cliques de mouse.

Por meio do uso da criptografia você pode:

proteger os dados sigilosos armazenados em seu computador, como o seu arquivo de senhas e a sua declaração de Imposto de Renda;

criar uma área (partição) específica no seu computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas; proteger seus backups contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias;

proteger as comunicações realizadas pela Internet, como os e-mails enviados/recebidos e as transações bancárias e comerciais realizadas.

Nas próximas seções são apresentados alguns conceitos de criptografia. Antes, porém, é importante que você se familiarize com alguns termos geralmente usados e que são mostrados na Tabela abaixo:

|  |  |
| --- | --- |
| **Termo** | **Significado** |
| Texto claro | Informação legível (original) que será protegida, ou seja, que será codificada |
| Texto codificado (cifrado) | Texto ilegível, gerado pela codificação de um texto claro |
| Codificar (cifrar) | Ato de transformar um texto claro em um texto codificado |
| Decodificar (decifrar) | Ato de transformar um texto codificado em um texto claro |
| Método criptográfico | Conjunto de programas responsável por codificar e decodificar informações |
| Chave | Similar a uma senha, é utilizada como elemento secreto pelos métodos criptográficos. Seu tamanho é geralmente medido em quantidade de *bits* |
| Canal de comunicação | Meio utilizado para a troca de informações |
| Criptoanálise | técnica utilizada para decifrar uma mensagem sem qualquer conhecimento dos detalhes de encriptação “Quebrar o código” |

Uma **cifra** é um algoritmo criptográfico, uma função matemática injetiva, que efetua as transformações entre o **texto claro** e o **texto cifrado.** A qualidade de uma cifra mede-se pelo tempo que permanece inquebrável, sendo do conhecimento geral, uma vez que o seu funcionamento interno é do conhecimento geral, o seu comportamento é controlado por uma **chave.**

**Cifra de Cesar**

Uso mais antigo que conhecemos de uma cifra foi feito por Júlio César no período da expansão romana. Consiste em Substituir cada letra do alfabeto por aquela que fica três posições adiante, como no exemplo abaixo:

**Texto Claro**: vulnerabilidade ponto fraco, falha ou fraqueza

**Text Cifrado**: Yxoqhudelolgdgh srqwr iudfr, idokd rx iudtxhcd

Da mesma forma que as letras foram trocadas na cifra de Cesar, elas podem ser substituídas com ordens aleatórias, inclusive utilizando símbolos e números. As cifras podem ainda utilizar em suas fórmulas para codificar mensagens permutações, matrizes (cifra de Hill), álgebra linear (Cifra de playfor) dentre outras funções matemáticas.

**Criptografia de chave simétrica e de chaves assimétricas**

De acordo com o tipo de chave usada, os métodos criptográficos podem ser subdivididos em duas grandes categorias: criptografia de chave simétrica e criptografia de chaves assimétricas.

**Criptografia de chave simétrica**: também chamada de criptografia de chave secreta ou única, utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados. Casos nos quais a informação é codificada e decodificada por uma mesma pessoa não há necessidade de compartilhamento da chave secreta. Entretanto, quando estas operações envolvem pessoas ou equipamentos diferentes, é necessário que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro (para não comprometer a confidencialidade da chave). Exemplos de métodos criptográficos que usam chave simétrica são: AES, Blowfish, RC4, 3DES e IDEA.

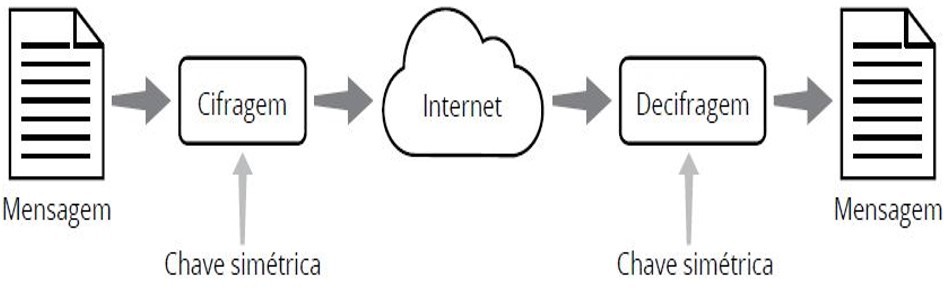
**Criptografia de chaves assimétricas**: também conhecida como criptografia de chave pública, utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono. Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se confidencialidade ou autenticação, integridade e não-repúdio. A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um smartcard ou um token. Exemplos de métodos criptográficos que usam chaves assimétricas são: RSA, DSA, ECC e Diffie-Hellman.

A criptografia de chave simétrica, quando comparada com a de chaves assimétricas, é a mais indicada para garantir a confidencialidade de grandes volumes de dados, pois seu processamento é mais rápido. Todavia, quando usada para o compartilhamento de informações, se torna complexa e pouco escalável, em virtude da:

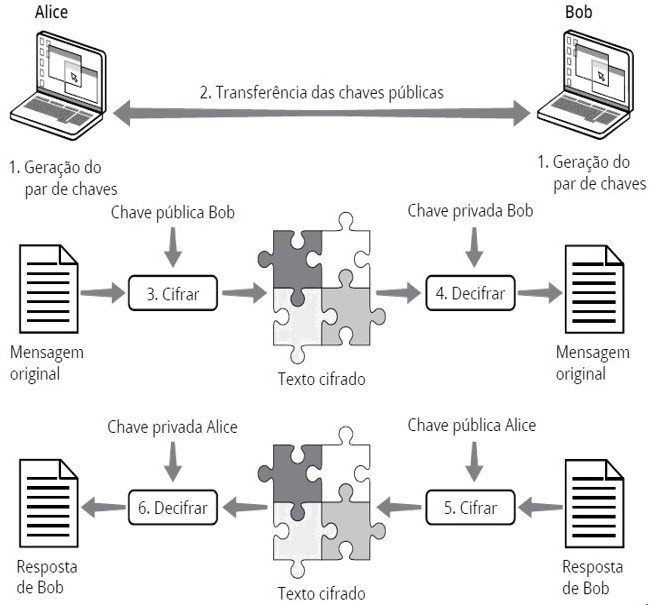
necessidade de um canal de comunicação seguro para promover o compartilhamento da chave secreta entre as partes (o que na Internet pode ser bastante complicado) e;

dificuldade de gerenciamento de grandes quantidades de chaves (imagine quantas chaves secretas seriam necessárias para você se comunicar com todos os seus amigos).





A criptografia de chaves assimétricas, apesar de possuir um processamento mais lento que a de chave simétrica, resolve estes problemas visto que facilita o gerenciamento (pois não requer que se mantenha uma chave secreta com cada um que desejar se comunicar) e dispensa a necessidade de um canal de comunicação seguro para o compartilhamento de chaves.



**Alice e Bob criam par de chaves individuais.**

**Alice e Bob trocam chaves públicas.**

**Alice escreve mensagem.**

**Alice usa chave pública de Bob para cifrar.**

**Alice envia resultado para Bob.**

**Bob usa sua chave privada para decifrar.**

**Bob escreve resposta, cifra com chave pública de Alice e envia para Alice.**

**Alice usa sua chave privada para decifrar a resposta.**

Para aproveitar as vantagens de cada um destes métodos, o ideal é o uso combinado de ambos, onde a criptografia de chave simétrica é usada para a codificação da informação e a criptografia de chaves assimétricas é utilizada para o compartilhamento da chave secreta (neste caso, também chamada de chave de sessão). Este uso combinado é o que é utilizado pelos navegadores Web e programas leitores de e-mails. Exemplos de uso deste método combinado são: SSL, PGP e S/MIME.

**Função de resumo (Hash)**

Uma função de resumo é um método criptográfico que, quando aplicado sobre uma informação, independente do tamanho que ela tenha, gera um resultado único e de tamanho fixo, chamado hash[1](https://cartilha.cert.br/criptografia/#footnote001).

**Você pode utilizar hash para:**

verificar a integridade de um arquivo armazenado em seu computador ou em seus backups;

verificar a integridade de um arquivo obtido da Internet (alguns sites, além do arquivo em si, também disponibilizam o hash correspondente, para que você possa verificar se o arquivo foi corretamente transmitido e gravado);

gerar assinaturas digitais

Para verificar a integridade de um arquivo, por exemplo, você pode calcular o hash dele e, quando julgar necessário, gerar novamente este valor. Se os dois hashes forem iguais então você pode concluir que o arquivo não foi alterado. Caso contrário, este pode ser um forte indício de que o arquivo esteja corrompido ou que foi modificado. Exemplos de métodos de hash são: SHA-1, SHA-256 e MD5.

1. O hash é gerado de tal forma que não é possível realizar o processamento inverso para se obter a informação original e que qualquer alteração na informação original produzirá um hash distinto. Apesar de ser teoricamente possível que informações diferentes gerem hashes iguais, a probabilidade disto ocorrer é bastante baixa.

**Assinatura digital**

A assinatura digital permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isto e que ela não foi alterada.

A assinatura digital baseia-se no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para codificar uma informação, então apenas seu dono poderia ter feito isto. A verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo.

Para contornar a baixa eficiência característica da criptografia de chaves assimétricas, a codificação é feita sobre o hash e não sobre o conteúdo em si, pois é mais rápido codificar o hash (que possui tamanho fixo e reduzido) do que a informação toda.

**Certificado digital**

Como dito anteriormente, a chave púbica pode ser livremente divulgada. Entretanto, se não houver como comprovar a quem ela pertence, pode ocorrer de você se comunicar, de forma cifrada, diretamente com um impostor.

Um impostor pode criar uma chave pública falsa para um amigo seu e enviá-la para você ou disponibilizá-la em um repositório. Ao usá-la para codificar uma informação para o seu amigo, você estará, na verdade, codificando-a para o impostor, que possui a chave privada correspondente e conseguirá decodificar. Uma das formas de impedir que isto ocorra é pelo uso de certificados digitais.

O certificado digital é um registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública. Ele pode ser emitido para pessoas, empresas, equipamentos ou serviços na rede (por exemplo, um site Web) e pode ser homologado para diferentes usos, como confidencialidade e assinatura digital.

Um certificado digital pode ser comparado a um documento de identidade, por exemplo, o seu passaporte, no qual constam os seus dados pessoais e a identificação de quem o emitiu. No caso do passaporte, a entidade responsável pela emissão e pela veracidade dos dados é a Polícia Federal. No caso do certificado digital esta entidade é uma Autoridade Certificadora (AC).

Uma AC emissora é também responsável por publicar informações sobre certificados que não são mais confiáveis. Sempre que a AC descobre ou é informada que um certificado não é mais confiável, ela o inclui em uma "lista negra", chamada de "Lista

de Certificados Revogados" (LCR) para que os usuários possam tomar conhecimento. A LCR é um arquivo eletrônico publicado periodicamente pela AC, contendo o número de série dos certificados que não são mais válidos e a data de revogação.

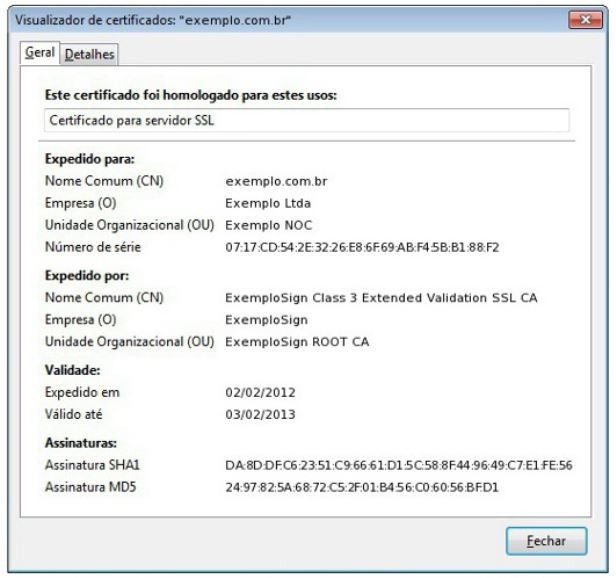
A Figura [abaixo](https://cartilha.cert.br/criptografia/#fig9.1) ilustra como os certificados digitais são apresentados nos navegadores Web. Note que, embora os campos apresentados sejam padronizados, a representação gráfica pode variar entre diferentes navegadores e sistemas operacionais. De forma geral, os dados básicos que compõem um certificado digital são:

versão e número de série do certificado;

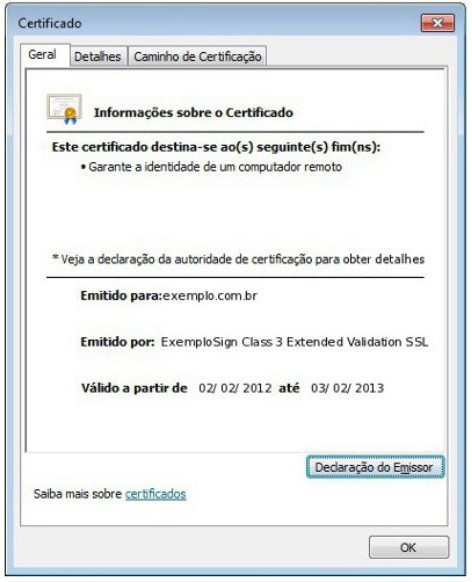
dados que identificam a AC que emitiu o certificado;

dados que identificam o dono do certificado (para quem ele foi emitido); chave pública do dono do certificado;

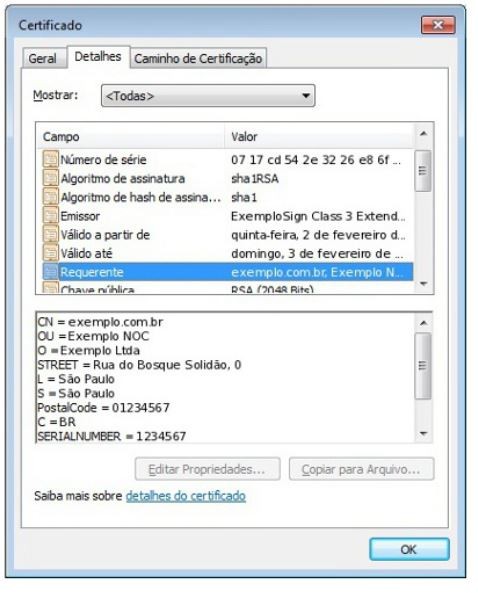
validade do certificado (quando foi emitido e até quando é válido); assinatura digital da AC emissora e dados para verificação da assinatura.





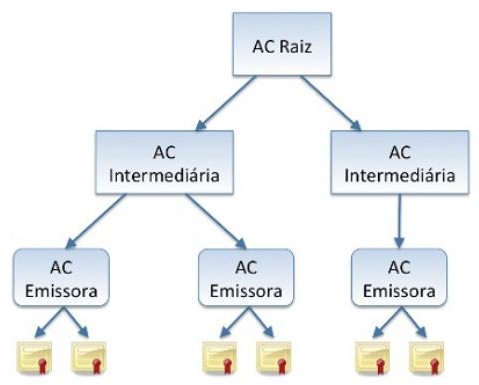






O certificado digital de uma AC é emitido, geralmente, por outra AC, estabelecendo uma hierarquia conhecida como "cadeia de certificados" ou "caminho de certificação", conforme ilustrado na Figura abaixo. A AC raiz, primeira autoridade da cadeia, é a âncora de confiança para toda a hierarquia e, por não existir outra AC acima dela, possui um certificado autoassinado (mais detalhes a seguir). Os certificados das ACs raízes publicamente reconhecidas já vêm inclusos, por padrão, em grande parte dos sistemas operacionais e navegadores e são atualizados juntamente com os próprios sistemas. Alguns exemplos de atualizações realizadas na base de certificados dos navegadores são: inclusão de novas ACs, renovação de certificados vencidos e exclusão de ACs não mais confiáveis.





Alguns tipos especiais de certificado digital que você pode encontrar são:

**Certificado autoassinado**: é aquele no qual o dono e o emissor são a mesma entidade. Costuma ser usado de duas formas:

**Legítima**: além das ACs raízes, certificados autoassinados também costumam ser usados por instituições de ensino e pequenos grupos que querem prover confidencialidade e integridade nas conexões, mas que não desejam (ou não podem) arcar com o ônus de adquirir um certificado digital validado por uma AC comercial.

**Maliciosa**: um atacante pode criar um certificado autoassinado e utilizar, por exemplo, mensagens de phishing (mais detalhes na lição phishing da unidade golpes e ataques na internet), para induzir os usuários a instalá-lo. A partir do momento em que o certificado for instalado no navegador, passa a ser possível estabelecer conexões cifradas com sites fraudulentos, sem que o navegador emita alertas quanto à confiabilidade do certificado.

**Certificado EV SSL (Extended Validation Secure Socket Layer)**

: certificado emitido sob um processo mais rigoroso de validação do solicitante. Inclui a verificação de que a empresa foi legalmente registrada, encontra-se ativa e que detém o registro do domínio para o qual o certificado será emitido, além de dados adicionais, como o endereço físico.

[…](https://www.youtube.com/watch?v=I3qEH3zIDr0)

[Criptografia Simétrica X Criptografi](https://www.youtube.com/watch?v=I3qEH3zIDr0)

**Programas de criptografia**

Para garantir a segurança das suas mensagens é importante usar programas leitores de e-mails com suporte nativo a criptografia (por exemplo, que implementam S/MIME

* Secure/Multipurpose Internet Mail Extensions) ou que permitam a integração de outros programas e complementos específicos para este fim.

Programas de criptografia, como o GnuPG2, além de poderem ser integrados aos programas leitores de e-mails, também podem ser usados separadamente para cifrar outros tipos de informação, como os arquivos armazenados em seu computador ou em mídias removíveis.

Existem também programas (nativos do sistema operacional ou adquiridos separadamente) que permitem cifrar todo o disco do computador, diretórios de arquivos e dispositivos de armazenamento externo (como pen-drives e discos), os quais visam preservar o sigilo das informações em caso de perda ou furto do equipamento.

1. <http://www.gnupg.org/>. O GnuPG não utiliza o conceito de certificados digitais emitidos por uma hierarquia de autoridades certificadoras. A confiança nas chaves é estabelecida por meio do modelo conhecido como "rede de confiança", no qual prevalece a confiança entre cada entidade.

**Vulnerabilidades Exploradas**

Ausência de programas de criptografia Utilização de chaves secretas óbvias ou fracas

Meio inseguro no compartilhamento de chaves simétricas Armazenamento de chave criptográfica em local desprotegido

Utilização de chave criptográfica em dispositivo inseguro (lan house, pc infectado com programa malicioso...)

Ausência de backup das chaves criptográficas

Contato utilizando engenharia social

**Prevenção**

Proteja seus dados:

utilize criptografia sempre que, ao enviar uma mensagem, quiser assegurar-se que somente o destinatário possa lê-la;

utilize assinaturas digitais sempre que, ao enviar uma mensagem, quiser assegurar ao destinatário que foi você quem a enviou e que o conteúdo não foi alterado;

só envie dados sensíveis após certificar-se de que está usando uma conexão segura;

utilize criptografia para conexão entre seu leitor de e-mails e os servidores de e- mail do seu provedor;

cifre o disco do seu computador e dispositivos removíveis, como disco externo e pen-drive. Desta forma, em caso de perda ou furto do equipamento, seus dados não poderão ser indevidamente acessados;

verifique o hash, quando possível, dos arquivos obtidos pela Internet (isto permite que você detecte arquivos corrompidos ou que foram indevidamente alterados durante a transmissão).

**Seja cuidadoso com as suas chaves e certificados**:

utilize chaves de tamanho adequado. Quanto maior a chave, mais resistente ela será a ataques de força bruta (mais detalhes na lição força bruta da unidade golpes e ataques na internet);

não utilize chaves secretas óbvias (mais detalhes na unidade golpes e ataques na internet);

certifique-se de não estar sendo observado ao digitar suas chaves e senhas de proteção;

utilize canais de comunicação seguros quando compartilhar chaves secretas; armazene suas chaves privadas com algum mecanismo de proteção, como por exemplo senha, para evitar que outra pessoa faça uso indevido delas;

preserve suas chaves. Procure fazer backups e mantenha-os em local seguro (se você perder uma chave secreta ou privada, não poderá decifrar as mensagens que dependiam de tais chaves);

tenha muito cuidado ao armazenar e utilizar suas chaves em computadores potencialmente infectados ou comprometidos, como em LAN houses, cybercafes, stands de eventos, etc;

se suspeitar que outra pessoa teve acesso à sua chave privada (por exemplo, porque perdeu o dispositivo em que ela estava armazenada ou porque alguém acessou indevidamente o computador onde ela estava guardada), solicite imediatamente a revogação do certificado junto à AC emissora.

**Seja cuidadoso ao aceitar um certificado digital**:

mantenha seu sistema operacional e navegadores Web atualizados (além disto contribuir para a segurança geral do seu computador, também serve para

manter as cadeias de certificados sempre atualizadas);

mantenha seu computador com a data correta. Além de outros benefícios, isto impede que certificados válidos sejam considerados não confiáveis e, de forma contrária, que certificados não confiáveis sejam considerados válidos;

ao acessar um site Web, observe os símbolos indicativos de conexão segura e leia com atenção eventuais alertas exibidos pelo navegador;

caso o navegador não reconheça o certificado como confiável, apenas prossiga com a navegação se tiver certeza da idoneidade da instituição e da integridade do certificado, pois, do contrário, poderá estar aceitando um certificado falso, criado especificamente para cometer fraudes.

X



[Curso em Segurança da Informação](https://mooc-seginfo.appspot.com/moocseg/)

[williamdasilvamelo@gmail.com](mailto:williamdasilvamelo@gmail.com) | [Dashboard](https://mooc-seginfo.appspot.com/moocseg/dashboard) | Sair

[Notificações](https://mooc-seginfo.appspot.com/moocseg/announcements) [**Curso**](https://mooc-seginfo.appspot.com/moocseg/course)[Progresso](https://mooc-seginfo.appspot.com/moocseg/student/home)

**Search**

[Curso](https://mooc-seginfo.appspot.com/moocseg/course) › [Unidade 2](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1) › Lição 1

# Unidade 2 - Programas Maliciosos - Malware [](https://mooc-seginfo.appspot.com/moocseg/dashboard?action=edit_unit&amp;key=1)



 **2.1 Vírus**

 [2.2 Worms](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=3)

**Vírus** 

 [2.3 Bot e Botnet](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=4)

 [2.4 Spyware](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=5)

 [2.5 Backdoor](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=6)

 [2.6 Cavalo de Tróia](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=7)

 [2.7](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

[Ransomware](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

 [2.8 Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=13)

 [2.9 Tutorial Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=43)

Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que permite inserir as seguintes cópias e se tornar parte de outros programas e arquivos. Para que possa tornar-se ativo e hereditário no processo de infecção, o vírus depende da execução do programa ou arquivo hospedado, ou seja, para que o seu computador seja infectado ou preciso que um programa já infectado seja executado.

O principal meio de propagação de vírus costuma ser os disquetes. Com o tempo, porém, essas mídias causam desuso e causam novas cirurgias,

como envio de email. Atualmente, como mídia removível usada novamente ou principal meio de propagação, mas não mais por disquetes, mas principalmente pelo uso de pen-drives.

Existem diferentes tipos de vírus. Alguns presos podem ocultar, infectar arquivos do disco e usar uma série de atividades sem o conhecimento do usuário. Há outros que permanecem inativos durante certos períodos, entrando em atividades apenas em dados usados. Alguns dos tipos de vírus mais comuns são:

**Vírus propagado por e-mail** : Recebido como um arquivo anexo em um e- mail cujo conteúdo tenta induzir o usuário a clicar sobre esse arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia registros para e-mails encontrados nas listas de contatos gravados no computador.

**Vírus de script:** escrito em linguagem de script, como VBScript e JavaScript, e recebido ao acessar uma página da Web ou por email, como um arquivo anexo ou como parte do próprio email escrito em formato HTML. Pode ser executado automaticamente, dependendo da configuração do navegador da Web e do programa leitor de e-mails do usuário.

**Vírus de macro** : tipo específico de vírus de script, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que usam esta linguagem como, por exemplo, os que compõem o Microsoft Office (Excel, Word e PowerPoint, entre outros).

**Vírus de telefone celular**: vírus que propaga celular para meio de tecnologia bluetooth ou de mensagens MMS (Multimedia Message Service). A infecção ocorre quando um usuário permite ou recebe um arquivo infectado e executa. Após infectar o celular, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, ativar ligar para telefones e drenar uma carga de bateria, além de tentar se propagar para outros celulares.

**Alguns exemplos interessantes de Vírus:**

Nome: **Melissa** Categoria: **Vírus** Criador: **David L. Smith**

Ano de lançamento: **1999**

Prejuízo causado: **1 bilhão de dólares**

O nome curioso desse vírus vem de uma dançarina de boate que trabalhava na Flórida, na qual o criador do vírus David L. Smith, gostava. O vírus

desligava todos os sistemas de e-mails por onde os e-mails infectados com o vírus passavam. Inicialmente ele foi usado em arquivos que contêm senhas de sites, como documentos do Word.

Nome: **CIH**

Categoria: **Vírus**

Criador: **Chen Ing Hau**

Ano de lançamento: **1998**

Prejuízo causado: **20 a 80 milhões de dólares**

O vírus CIH, também conhecido como Chernobyl, foi um dos vírus mais devastadores já conhecidos. Diferentemente dos outros vírus que causam danos leves e apenas se reproduzem, esse vírus literalmente destrói todos os dados do computador. Em alguns casos, até destruir os dados do BIOS, transformando qualquer PC em sucata. Seu poder de propagar foi neutralizado com uma atualização da Microsoft, já que ele atacava apenas versões antigas do Windows, como 95, 98 e Millenium.

Nome: **Love You**

Categoria: **Vírus**

Criador: **Desconhecido. Estima-se que alguém das Filipinas**

Ano de lançamento: **2000**

Prejuízo estimado: **Entre 5,5 a 8,7 bilhões de dólares**

De todos os vírus que já existiram, este foi o que mais trouxe problemas e prejuízos ao redor do mundo. O motivo é óbvio: todo mundo abriria um e- mail cujo assunto é “Eu te amo”, o nome do vírus, em inglês. Em maio de 2000, estima-se que 50 milhões de computadores foram infectados. Só que além dos usuários comuns, grandes órgãos dos governos ao redor do mundo também tiveram seus PCs afetados pelo vírus. Vários deles, como a CIA, tiveram que desligar o seu sistema de e-mail para diminuir o impacto da disseminação do vírus.

[Próxima página](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=3)

X



[Curso em Segurança da Informação](https://mooc-seginfo.appspot.com/moocseg/)

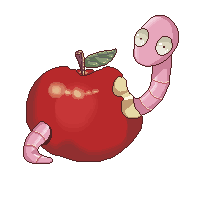
[williamdasilvamelo@gmail.com](mailto:williamdasilvamelo@gmail.com) | [Dashboard](https://mooc-seginfo.appspot.com/moocseg/dashboard) | Sair

[Notificações](https://mooc-seginfo.appspot.com/moocseg/announcements) [**Curso**](https://mooc-seginfo.appspot.com/moocseg/course)[Progresso](https://mooc-seginfo.appspot.com/moocseg/student/home)

**Search**

[Curso](https://mooc-seginfo.appspot.com/moocseg/course) › [Unidade 2](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1) › Lição 2

# Unidade 2 - Programas Maliciosos - Malware [](https://mooc-seginfo.appspot.com/moocseg/dashboard?action=edit_unit&amp;key=1)



 [2.1 Vírus](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=2)

 **2.2 Worms**

**Worms** 

 [2.3 Bot e Botnet](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=4)

 [2.4 Spyware](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=5)

 [2.5 Backdoor](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=6)

 [2.6 Cavalo de Tróia](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=7)

 [2.7](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

[Ransomware](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

 [2.8 Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=13)

 [2.9 Tutorial Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=43)

Worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Worms são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores.

O processo de propagação e infecção dos worms ocorre da seguinte maneira:

1. **Identificacão dos computadores alvos:** após infectar um computador, o worm tenta se propagar e continuar o processo de infecção. Para isto, necessita identificar os computadores alvos para os quais tentará se copiar, o que pode ser feito de uma ou mais das seguintes maneiras:

efetuar varredura na rede e identificar computadores ativos;

aguardar que outros computadores contatem o computador infectado; utilizar listas, predefinidas ou obtidas na Internet, contendo a identificação dos alvos;

utilizar informações contidas no computador infectado, como arquivos

de configuração e listas de endereços de e-mail

1. **Envio das cópias:** após identificar os alvos, o worm efetua cópias de si mesmo e tenta enviá-las para estes computadores, por uma ou mais das seguintes formas:

como parte da exploração de vulnerabilidades existentes em programas instalados no computador alvo;

anexadas a e-mails;

via canais de IRC (Internet Relay Chat);

via programas de troca de mensagens instantâneas;

incluídas em pastas compartilhadas em redes locais ou do tipo P2P (Peer to Peer).

1. **Ativação das cópias**: após realizado o envio da cópia, o worm necessita ser executado para que a infecção ocorra, o que pode acontecer de uma ou mais das seguintes maneiras:

Imediatamente após ter sido transmitido, pela exploração de vulnerabilidades em programas sendo executados no computador alvo no momento do recebimento da cópia;

diretamente pelo usuário, pela execução de uma das cópias enviadas ao seu computador;

pela realização de uma ação específica do usuário, a qual o worm está condicionado como, por exemplo, a inserção de uma mídia removível.

1. **Reinício do processo**: após o alvo ser infectado, o processo de propagação e infecção recomeça, sendo que, a partir de agora, o computador que antes era o alvo passa a ser também o computador originador dos ataques.

Alguns exemplos interessantes de Worms:

Nome: **Morris**

Categoria: **Worm**

Criador: **Robert Morris**

Ano de lançamento: **1988**

Prejuízo causado: **entre 10 e 100 milhões de dólares**

Esse foi um worm criado sem más intenções, mas foi capaz de mostrar como um apenas um código pode se tornar uma ameaça muito perigosa. Ele foi criado por Robert Morris para medir o tamanho da Internet. O problema do worm é que ele tinha um erro que infectava o computador várias vezes, o que lhes causava também um ataque de negação de serviço (neste ataque, o vírus sobrecarrega as vias de comunicação do sistema, obrigando algumas instruções a “esperarem na fila de tarefas”. O problema é que a espera, depois de um tempo, inutiliza o computador).

Nome: **Code Red**

Categoria: **Worm**

Criador: **Desconhecido. Provavelmente originou-se na China**

Ano de lançamento: **2001**

Prejuízo causado: **2 bilhões de dólares**

O worm Code Red aproveitava-se de uma vulnerabilidade de estouro de buffer dos servidores Microsoft IIS e se replicava para outros servidores IIS (buffer é uma região da memória temporária utilizada para escrever e ler dados antes deles serem guardados permanentemente). Quando acontecia o estouro do buffer, o servidor desligava. Os sites guardados nesses servidores, que foram afetados pelo worm, passavam então a exibir a mensagem “Hacked by Chinese!” ("Hackeado por Chinês", em tradução literal). O nome Code Red surgiu quando os pesquisadores da eEye Digital Security descobriram o worm, e naquele momento estavam tomando uma bebida chamada "Code Red Mountain Dew".

Nome: **Slammer** Categoria: **Worm** Criador: **Desconhecido** Ano de lançamento: **2003**

Prejuízo causado: Desconhecido. Sabe-se que a Coreia do Sul ficou sem internet por 12 horas.

Esse worm se aproveitava de uma vulnerabilidade de estouro de buffer no Microsoft SQL Server, um aplicativo famoso para gerenciamento de bancos de dados. Uma vez instalado, ele causava um ataque de negação de serviço, fazendo com que os bancos de dados não respondessem e

causassem grande lentidão na Internet. O worm se replicava e atacava todos os servidores SQL Server que tinham a mesma vulnerabilidade, causando um efeito cascada no qual os sistemas passavam a não responder mais. Estima-se que cerca de 75.000 computadores foram afetados em apenas 10 minutos. Ele foi tão agressivo e rápido que muitos, na época, pensaram que era um ataque coordenado por um grupo hacker.

Nome: **Nimda** Categoria: **Worm** Criador: **Desconhecido** Ano de lançamento: **2001**

Prejuízo causado: **Desconhecido**

O worm Nimda usava vários métodos para se espalhar, como e-mail, as redes internas, navegação de sites e backdoors (portas de conexão com a Internet) deixados por outros vírus - e por isso ele causou uma lentidão absurda na Internet. Por essa habilidade de se espalhar, o Nimda foi considerado o worm mais rápido até o momento, precisando de apenas 22 minutos para entrar na Internet e se tornar o vírus 'mais espalhado do mundo'. O nome Nimda vem da palavra “admin” escrita ao contrário, referente aos usuários administradores de servidores.

Nome: **Blaster**

Categoria: **Worm**

Criador: **Grupo hacker chinês Xfocus**

Ano de lançamento: **2003**

Prejuízo: **entre 2 a 10 bilhões de dólares**

O worm foi criado com a intenção de atacar os sistemas Windows da Microsoft. Além de atacar o sistema operacional, o worm continha a seguinte mensagem para a empresa: "Billy Gates why do you make this possible? Stop making money and fix your software!!" (em tradução literal: “Bill Gates por que você fez isso ser 'possível'? Pare de fazer dinheiro e corrija seu software!”).

Nome: **Sasser** Categoria: **Worm** Criador: **Sven Jaschan**

Ano de lançamento: **2004**

Prejuízo: **10 milhões de dólares**

O Sasser também atacou várias máquinas com o Windows. Para isso, usou uma vulnerabilidade de segurança na porta de rede, conectando-se a outras máquinas e se espalhando pela Internet. Só que não foi por isso que ele ficou conhecido. O worm afetou várias empresas, como a Delta Airlines, que teve que interromper seus voos por conta da infecção. A Guarda Costeira da Inglaterra teve seus serviços de mapas interrompidos, e a agência de notícias France-Press também teve as suas comunicações com os satélites interrompidas.

Nome: **Storm** Categoria: **Worm** Criador: **Desconhecido**

Ano de lançamento: **2007**

Prejuízo: **Não estimado**

O Storm teve um modo de propagação curioso: ele mandava e-mails com assuntos polêmicos ou sensacionalistas, como “Genocídio de muçulmanos britânico” ou “Fidel Castro faleceu”. Por ser um worm mais moderno, o Storm construiu uma verdadeira "botnet" - ou seja, ele usava o seu computador infectado para realizar ações programadas pelo worm, como ataques a determinados sites. Deatlhe: os computadores infectados comunicavam-se entre si para melhorar as formas de ataque.

[…](https://www.youtube.com/watch?v=5C0I2DNvvrg)

[Minuto do Concurseiro - Virus vs. Worm - Professora Nan](https://www.youtube.com/watch?v=5C0I2DNvvrg)

[Página anterior](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=2)

[Próxima página](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=4)

X

[Curso em Segurança da Informação](https://mooc-seginfo.appspot.com/moocseg/)

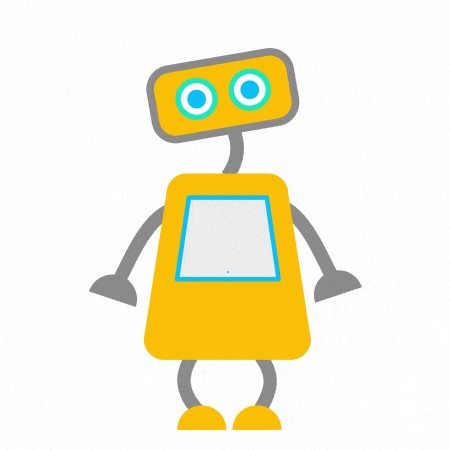
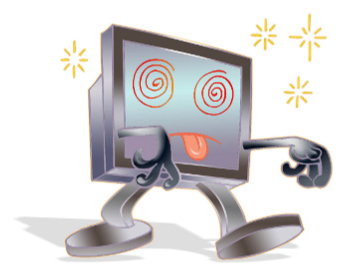
[williamdasilvamelo@gmail.com](mailto:williamdasilvamelo@gmail.com) | [Dashboard](https://mooc-seginfo.appspot.com/moocseg/dashboard) | Sair

[Notificações](https://mooc-seginfo.appspot.com/moocseg/announcements) [**Curso**](https://mooc-seginfo.appspot.com/moocseg/course)[Progresso](https://mooc-seginfo.appspot.com/moocseg/student/home)

[Curso](https://mooc-seginfo.appspot.com/moocseg/course) › [Unidade 2](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1) › Lição 3

**Search**

**Unidade 2 - Programas Maliciosos - Malware** [](https://mooc-seginfo.appspot.com/moocseg/dashboard?action=edit_unit&amp;key=1)



 [2.1 Vírus](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=2)

 [2.2 Worms](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=3)

 **2.3 Bot e Botnet**

 [2.4 Spyware](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=5)

 [2.5 Backdoor](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=6)

Bot e Botnet 

 [2.6 Cavalo de Tróia](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=7)

 [2.7 Ransomware](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

 [2.8 Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=13)

 [2.9 Tutorial Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=43)

Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores. A comunicação entre o invasor e o computador infectado pelo bot pode ocorrer via canais de IRC (Internet Relay Chat), servidores Web e redes do tipo P2P, entre outros meios. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar spam.

Um computador infectado por um bot costuma ser chamado de zumbi (zombie computer), pois pode ser controlado remotamente, sem o conhecimento do seu dono. Também pode ser chamado de spam zombie quando o bot instalado o transforma em um servidor de e-mails e o utiliza para o envio de

spam. Entretanto, zumbis podem ser também: dispositivos móveis (tablets, smartphones, celulares), equipamentos de rede ( roteadores, modems)

Botnet é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots. Quanto mais zumbis participarem da botnet mais potente ela será. O atacante que a controlar, além de usá-la para seus próprios ataques, também pode alugá-la para outras pessoas ou grupos que desejem que uma ação maliciosa específica seja executada.

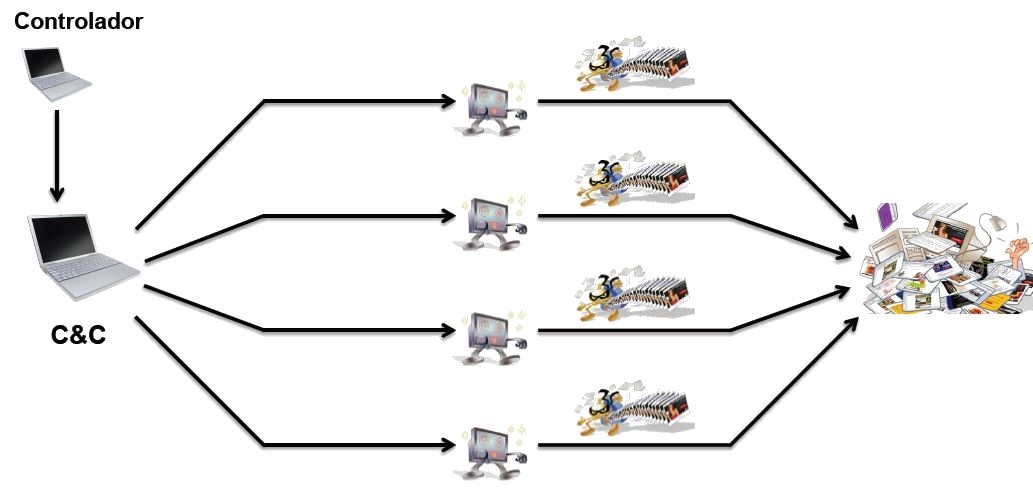


Algumas das ações maliciosas que costumam ser executadas por intermédio de botnets são: ataques de negação de serviço, propagação de códigos maliciosos (inclusive do próprio bot), coleta de informações de um grande número de computadores, envio de spam e camuflagem da identidade do atacante (com o uso de proxies instalados nos zumbis), desativação de mecanismos de segurança (antivírus, antimalware, antispam).

O esquema simplificado apresentado a seguir exemplifica o funcionamento básico de uma botnet:

1. Um atacante propaga um tipo específico de bot na esperança de infectar e conseguir a maior quantidade possível de zumbis;
2. os zumbis ficam então à disposição do atacante, agora seu controlador, à espera dos comandos a serem executados;
3. quando o controlador deseja que uma ação seja realizada, ele envia aos zumbis os comandos a serem executados, usando, por exemplo, redes do tipo P2P ou servidores centralizados;
4. os zumbis executam então os comandos recebidos, durante o período predeterminado pelo controlador;
5. quando a ação se encerra, os zumbis voltam a ficar à espera dos próximos comandos a serem executados.

O controlador da botnet (botmaster) usa um servidor chamado command and control (C&C) para se comunicar com os zumbis.



**Conferir resposta**

1. - Zumbis ficam à espera dos comandos a serem executados
2. - Controlador envia ao C&C os comandos a serem executados (exemplo: envio de spam)
3. - C&C repassa os comandos aos zumbis
4. - Zumbis executam os comandos pelo tempo determinado

O é um programa capaz de se propagar automaticamente pelas *Um ponto* redes, enviando cópias de si mesmo de computador para computador. É notadamente responsável por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costuma propagar e, como consequência, pode afetar o desempenho da rede e a utilização do computador.Assinale a alternativa que CORRETAMENTE preenche a lacuna do texto acima.

Trojan Keylogger Vírus Worm Spyware

[Página anterior](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=3)

[Próxima página](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=5)

X



[Curso em Segurança da Informação](https://mooc-seginfo.appspot.com/moocseg/)

[williamdasilvamelo@gmail.com](mailto:williamdasilvamelo@gmail.com) | [Dashboard](https://mooc-seginfo.appspot.com/moocseg/dashboard) | Sair

[Notificações](https://mooc-seginfo.appspot.com/moocseg/announcements) [**Curso**](https://mooc-seginfo.appspot.com/moocseg/course)[Progresso](https://mooc-seginfo.appspot.com/moocseg/student/home)

**Search**

[Curso](https://mooc-seginfo.appspot.com/moocseg/course) › [Unidade 2](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1) › Lição 4

# Unidade 2 - Programas Maliciosos - Malware [](https://mooc-seginfo.appspot.com/moocseg/dashboard?action=edit_unit&amp;key=1)



 [2.1 Vírus](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=2)

 [2.2 Worms](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=3)

##### Spyware 

 [2.3 Bot e Botnet](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=4)

 **2.4 Spyware**

 [2.5 Backdoor](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=6)

 [2.6 Cavalo de Tróia](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=7)

 [2.7](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

[Ransomware](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

 [2.8 Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=13)

 [2.9 Tutorial Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=43)

**Spyware** é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas.

Pode ser considerado de uso:

**Legítimo**: quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado.

**Malicioso**: quando executa ações que podem comprometer a privacidade

do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha), dados referentes a pagamentos, cartões de crédito.

Os spywares podem colher informações do registro dos URLs dos sites visitados, das palavras-chave introduzidas nos motores de busca, da análise das compras realizadas pela Internet, monitorando os hábitos dos usuários. Essas informações, normalmente são comercializadas por traçarem um perfil de consumo do usuário. Assim, algumas empresas utilizam-se de spywares para anunciar bens e serviços susceptíveis de compra.

Esses programas instalam-se, geralmente, junto com outros softwares, isso permite a seus autores rentabilizarem o seu sistema com a venda de informações, estatísticas para assim poder distribuir seu software gratuitamente. Este é um modelo econômico no qual a gratuidade é obtida através da cessão de dados pessoais, que podem ocorrer legalmente com consentimento do usuário (aceitando um contrato de licença) ou ilegalmente sem o consentimento e autorização do usuário.

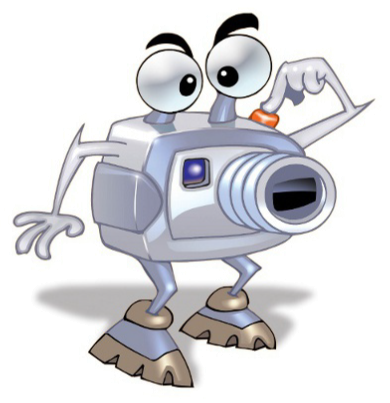
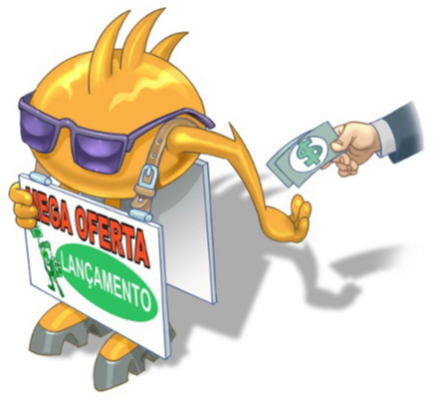
Alguns tipos específicos de programas spyware são:

**Keylogger:** capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação em muitos casos, é condicionada a uma ação

prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking**.**

**Screenlogger:** Similar ao keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos

usuários em teclados virtuais, disponíveis principalmente em sites de Internet Banking.



**Adware**: projetado especificamente para apresentar propagandas. Pode ser usado para fins

legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.

[Spyware](https://www.youtube.com/watch?v=DfG6HOABGx4)

[Página anterior](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=4)

[Próxima página](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=6)

X



[Curso em Segurança da Informação](https://mooc-seginfo.appspot.com/moocseg/)

[williamdasilvamelo@gmail.com](mailto:williamdasilvamelo@gmail.com) | [Dashboard](https://mooc-seginfo.appspot.com/moocseg/dashboard) | Sair

[Notificações](https://mooc-seginfo.appspot.com/moocseg/announcements) [**Curso**](https://mooc-seginfo.appspot.com/moocseg/course)[Progresso](https://mooc-seginfo.appspot.com/moocseg/student/home)

**Search**

[Curso](https://mooc-seginfo.appspot.com/moocseg/course) › [Unidade 2](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1) › Lição 5

# Unidade 2 - Programas Maliciosos - Malware [](https://mooc-seginfo.appspot.com/moocseg/dashboard?action=edit_unit&amp;key=1)



 [2.1 Vírus](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=2)

 [2.2 Worms](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=3)

##### Backdoor 

 [2.3 Bot e Botnet](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=4)

 [2.4 Spyware](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=5)

 **2.5 Backdoor**

 [2.6 Cavalo de Tróia](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=7)

 [2.7](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

[Ransomware](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

 [2.8 Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=13)

 [2.9 Tutorial Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=43)

***Backdoor*** é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que exploram vulnerabilidades existentes nos programas instalados no computador para invadi-lo.

Após incluído, o *backdoor* é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na

realização da invasão ou infecção e, na maioria dos casos, sem que seja notado.



**Conferir resposta**

A forma usual de inclusão de um *backdoor* consiste na disponibilização de um novo serviço ou na substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitem o acesso remoto. Programas de administração remota, como BackOrifice, NetBus, SubSeven, VNC e Radmin, se mal configurados ou utilizados sem o consentimento do usuário, também podem ser classificados como *backdoors*.

Há casos de *backdoors* incluídos propositalmente por fabricantes de programas, sob alegação de necessidades administrativas. Esses casos constituem uma séria ameaça à segurança de um computador que contenha um destes programas instalados pois, além de comprometerem a privacidade do usuário, também podem ser usados por invasores para acessarem remotamente o computador.

Existem diversos tipos de códigos maliciosos, entre eles o spyware. *Um ponto*

Acerca desse assunto, é correto afirmar que spyware consiste em:

Programa que além de projetar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, sem o conhecimento do usuário.

Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para esse fim.

Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

Programa ou parte de um programa de computador, normalmente malicioso, que se propaga, inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos.

Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

[Página anterior](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=5)

[Próxima página](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=7)

X



[Curso em Segurança da Informação](https://mooc-seginfo.appspot.com/moocseg/)

[williamdasilvamelo@gmail.com](mailto:williamdasilvamelo@gmail.com) | [Dashboard](https://mooc-seginfo.appspot.com/moocseg/dashboard) | Sair

[Notificações](https://mooc-seginfo.appspot.com/moocseg/announcements) [**Curso**](https://mooc-seginfo.appspot.com/moocseg/course)[Progresso](https://mooc-seginfo.appspot.com/moocseg/student/home)

**Search**

[Curso](https://mooc-seginfo.appspot.com/moocseg/course) › [Unidade 2](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1) › Lição 6

# Unidade 2 - Programas Maliciosos - Malware [](https://mooc-seginfo.appspot.com/moocseg/dashboard?action=edit_unit&amp;key=1)

 [2.1 Vírus](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=2)

 [2.2 Worms](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=3)



**Cavalo de Tróia** 

**Cavalo de troia1**, trojan ou trojan-horse, é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

Exemplos de trojans são programas que você recebe ou obtém de sites na Internet e que parecem ser apenas cartões virtuais animados, álbuns de

 [2.3 Bot e Botnet](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=4)

 [2.4 Spyware](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=5)

 [2.5 Backdoor](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=6)

 **2.6 Cavalo de Tróia**

 [2.7](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

[Ransomware](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

 [2.8 Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=13)

 [2.9 Tutorial Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=43)

fotos, jogos e protetores de tela, entre outros. Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador. Assim, o programa que se apresenta contendo uma determinada finalidade, que realmente tem, mas adicionalmente e de forma secreta, possui uma segunda função cujo objetivo é abrir o computador para invasões, acessos remotos ou roubo de informações (senhas, por exemplo).

Trojans também podem ser instalados por atacantes que, após invadirem um computador, alteram programas já existentes para que, além de continuarem a desempenhar as funções originais, também executem ações maliciosas.

Há diferentes tipos de trojans, classificados2 de acordo com as ações maliciosas que costumam executar ao infectar um computador. Alguns destes tipos são:

**Trojan Downloader**: instala outros códigos maliciosos, obtidos de sites na Internet.

**Trojan Dropper**: instala outros códigos maliciosos, embutidos no próprio código do trojan.

**Trojan Backdoor**: inclui backdoors, possibilitando o acesso remoto do atacante ao computador.

**Trojan DoS**: instala ferramentas de negação de serviço e as utiliza para desferir ataques.

**Trojan Destrutivo**: altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.

**Trojan Clicker**: redireciona a navegação do usuário para sites específicos, com o objetivo de aumentar a quantidade de acessos a estes sites ou apresentar propagandas.

**Trojan Proxy**: instala um servidor de proxy, possibilitando que o computador seja utilizado para navegação anônima e para envio de spam.

**Trojan Spy**: instala programas spyware e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante.

**Trojan Banker ou Bancos**: coleta dados bancários do usuário, através da instalação de programas spyware que são ativados quando sites de Internet Banking são acessados. É similar ao Trojan Spy porém com objetivos mais específicos.

O Cavalo de Tróia distingue-se por não replicar, por não infectar outros arquivos ou propagar cópias de si mesmo automaticamente. O arquivo

precisa ser executado, as seguintes ações maliciosas podem ser executadas:

1. alteração ou destruição de arquivos
2. furto de senhas e outras informações sensíveis
3. inclusão de backdoors, permitindo controle total sobre o computador

[Cavalo de Troia ou Trojan Horse - Dicionário de Informática](https://www.youtube.com/watch?v=LRgo4F4HxWo)

1. O "Cavalo de Troia", segundo a mitologia grega, foi uma grande estátua, utilizada como instrumento de guerra pelos gregos para obter acesso à cidade de Troia. A estátua do cavalo foi recheada com soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos gregos e a dominação de Troia.
2. Esta classificação baseia-se em coletânea feita sobre os nomes mais comumente usados pelos programas antimalware.

[Página anterior](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=6)

[Próxima página](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

X

[Curso em Segurança da Informação](https://mooc-seginfo.appspot.com/moocseg/)

[williamdasilvamelo@gmail.com](mailto:williamdasilvamelo@gmail.com) | [Dashboard](https://mooc-seginfo.appspot.com/moocseg/dashboard) | Sair

[Notificações](https://mooc-seginfo.appspot.com/moocseg/announcements) [**Curso**](https://mooc-seginfo.appspot.com/moocseg/course)[Progresso](https://mooc-seginfo.appspot.com/moocseg/student/home)

[Curso](https://mooc-seginfo.appspot.com/moocseg/course) › [Unidade 2](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1) › Lição 7

**Search**

**Unidade 2 - Programas Maliciosos - Malware** [](https://mooc-seginfo.appspot.com/moocseg/dashboard?action=edit_unit&amp;key=1)

 [2.1 Vírus](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=2)



**Ransomware** 

**Ransomware** é uma categoria que corresponde a todo tipo de código malicioso que exige o pagamento de um resgate para recuperar a informação do usuário. Uma vez que infectou o equipamento, esse malware utiliza diferentes mecanismos para tornar os dados inacessíveis pelo usuário, com o objetivo de extorquir e exigir o pagamento de uma quantia de dinheiro em troca do acesso à informação novamente. É importante entender que o ransomware no geral não rouba e nem abre o conteúdo da informação, mas sim bloqueia seu acesso. As primeiras variantes de ransomware

bloqueavam a tela do usuário e utilizavam diferentes formas para fazer com que as

 [2.2 Worms](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=3)

 [2.3 Bot e Botnet](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=4)

 [2.4 Spyware](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=5)

 [2.5 Backdoor](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=6)

 [2.6 Cavalo de Tróia](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=7)

 **2.7**

**Ransomware**

 [2.8 Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=13)

 [2.9 Tutorial Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=43)

pessoas acreditassem que havia um problema ou haviam cometido algum delito e deveriam pagar para solucioná-lo. Atualmente, existem novas variantes que utilizam algorítmos complexos de criptografia para bloquear a informação e solicitar dinheiro, para em troca, recuperá-la. Diferente de outros códigos maliciosos, o ransomware não busca passar despercebido, muito pelo contrário: ele deseja chamar a atenção dos usuários infectados. Talvez muitas empresas foram infectadas com códigos maliciosos e nunca tenham percebido ou se passaram vários dias até que tenha sido detectada a infecção. Além disso, o ransomware se detecta no momento, já que o mesmo código cria um alerta avisando o usuário que sua informação se encontra bloqueada e que ele deve pagar pelo resgate.

Existem duas variantes principais desse código malicioso usado para extorquir suas vítimas. Por um lado, o ransomware de bloqueio de tela, mais conhecido como “lockscreen”, que impede o acesso ao equipamento. Por outro lado, está o tipo de ransomware que utiliza a criptografia, chamado de “cryptolockers”, que criptografam a informação dentro do equipamento, impedindo o acesso aos arquivos.

**Lockscreen**: O ransomware do tipo lockscreen é caracterizado por impedir o acesso e o uso do equipamento por meio de uma tela de bloqueio, impossibilitando qualquer ação para fechá-la, abrir o administrador de tarefas, os navegadores web ou qualquer outra parte do sistema. Nessa tela geralmente aparece uma mensagem em que se explica o ocorrido e se solicita o pagamento do resgate. Dado que essa variante não criptografa os arquivos, nesses casos a informação poderia ser recuperada, já que é possível extrair o disco rígido e logo limpar o equipamento dessa infecção. Por essa mesma razão, esse malware costuma fazer uso de enganos e truques de engenharia social para persuadir o usuário para que ele pague o resgate.

**Cryptolockers**: O ransomware do tipo criptográfico, por sua vez, utiliza diversos algorítimos de criptografia para bloquear o acesso aos arquivos do usuário. Uma vez que ele se apodera de um sistema, se inicia uma mudança na estrutura dos arquivos e documentos, de maneira que só seria possível voltar a ler ou utilizá-los se fossem restaurados a seu estado original, o que requer o uso de uma chave conhecida somente pelos cibercriminosos. Na maiorira dos casos, o ataque afeta somente certos arquivos, sendo os do office os mais prejudicados. Uma vez finalizada a infecção, aparece uma tela que indica que os arquivos foram criptografados e explicando ao usuário o processo de pagamento em dinheiro em troca da chave para descriptografar a informação.

Formas de propagação:

**Mensagens falsas no email** - Enganam o usuário para fazer com que ele baixe um arquivo, seja esse documento anexado no e-mail ou através de um link na web. Esses arquivos maliciosos costumam ser trojans que aparentam ser documentos de texto ou imagens inofensivas, porém ao abrí-los se inicia o download do ransomware que finalmente bloqueia o equipamento e os arquivos do usuário.

**Download de arquivos em redes p2p ou sites de software pirata** - Muitos desses sites ou arquivos prometem algum software gratuito ou cracks para evadir verificações de licenciamento. Esse tipo de programa costuma solicitar que seja desabilitada a proteção antivírus, o que torna ainda mais fácil infectar o equipamento

É possível recuperar os arquivos?

Naturalmente, se você conta com a chave mestra será possível descriptografar os documentos, não obstante, conseguir a chave sem antes ter de pagar os cibercriminosos é complexo. Na maioria das vezes isso se mostra quase inviável, ainda mais se o algorítimo é forte; a chave não pode ser obtida a partir do código do malware; e a chave mestra é única para cada vítima e funciona somente para um equipamento.

No início de 2014 surgiram diversas famílias de ransomware para dispositivos Android, faziam com que aparecesse uma tela com uma mensagem falsa da polícia nacional, ou ainda do FBI. Essa tela indicava ao usuário que o equipamento havia sido bloqueado por conter material ilegal, como pornografia infantil, software pirata ou conteúdo com direitos autorais, e que era necessário pagar uma “multa” para restaurar o acesso normal. Utilizavam ainda, técnicas de engenharia social, incluindo garantir que o usuário era espiado pela câmera, para conseguir maior credibilidade e aumentar as chances de receber o dinheiro.

**Pagar ou não pagar?**

**Não é recomendado** pagar o resgate e não é interessante aceitar as demandas dos atacantes, por pelo menos três razões concretas:

Mesmo algumas vezes ao pagar o resgate se restaura o acesso aos dados, a verdade é que se está negociando com um cibercriminoso do outro lado, o qual não sabemos a identidade, nem temos a chance de econtrá- lo. Portanto, não existe nenhuma garantia de que realmente serão enviadas as chaves de descriptografia. Houveram casos em que não foi possível recuperar a informação, já que o criminoso jamais respondeu depois do pagamento do resgate, ou até mesmo solicitou o pagamento três vezes antes de realmente devolver o acesso aos dados.

Aceitar essas demandas só contribui para que esse tipo de ação por meio do ransomware seja cada vez mais rentável para os atacantes, e portanto, eles irão aperfeiçoando suas técnicas e se adptando a novos cenários. Se as vítimas possuem backup de seus dados e estão prevenidas, não será necessário que paguem o resgate, e isso vai enfraquecendo os esforços dos cibercriminosos.

O pagamento do resgate não significa que o usuário estará fora de perigo. Os atacantes podem deixar o malware no equipamento, já que agora sabem que está disposto à pagar dinheiro para recuperar o acesso ao equipamento ou aos dados. Resumindo, poderia voltar a ser o objetivo de outro ataque futuramente.

**Alguns exemplos interessantes de Ransomware:**

**WannaCryptor**

* Se tornou popular pelo nome **de WannaCry** (em português “quer chorar”), criptografa os arquivos do equipamento infectado utilizando uma combinação de algorítimos AES-128 e RSA-2048, o que faz com que seja impossível sua

recuperação por meio de técnicas de análise. No entanto, o que fez com que o ataque se tornasse realmente escandaloso foi sua capacidade de propagação, de maneira similar a um worm, através das redes dos equipamentos infectados, utilizando uma vulnerabilidade no protocolo de arquivos compartilhados do Windows.

**Simplocker** - Escaneia o cartão SD do dispositivo e criptografa os arquivos utilizando o algorítimo AES.

**Recomendações contra Ransomware:**

Não abrir arquivos anexados nem abrir links de e-mails desconhecidos ou não esperados

Manter os sistemas atualizados constantemente Não baixar aplicativos de fóruns ou lojas não oficiais

Manter o equipamento atualizado e obter uma solução de segurança.

Efetuar cópia de backup - Contar com uma cópia dos arquivos críticos é muito importante, para caso haja perda da informação, especialmente porque existem diversas causas pelas quais um usuário poderia passar por esse problema.

Educação em segurança da informação

[Tipos de Vírus para Computadores](https://www.youtube.com/watch?v=GK69-u1stJY)



Um Técnico de Informática está analisando como recursos de diversas pragas *Um ponto* virtuais (malwares), para executar a instalação do antivírus adequado. Dentre as características específicas por ele analisadas, estão: I. Programa que, além de executar as funções para as quais foram executadas, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário. Um exemplo é um programa que recebe ou obtém sites na Internet e que parece ser inofensivo. Esse programa geralmente consiste em um único arquivo e é explicitamente executado para que seja instalado no computador. II. Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído na ação de outros códigos maliciosos, que podem afetar o computador ou atacantes que exploram vulnerabilidades existentes nos programas utilizados no computador. Após incluído, ele é



usado para garantir o acesso futuro ao computador comprometido, permitir que ele seja acessado remotamente, caso haja necessidade de executar novamente os métodos de execução de invasão ou infecção e, na maioria dos casos, sem que seja notado. III Programa que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia. O atacante exige pagamento de resgate para restabelecer o acesso ao usuário. As descrições acima são, corretas e respectivamente, correspondentes a

Worm, backdoor e vírus

Bot, Rootkit e cavalo de Tróia (Trojan) Vírus, spyware e rootkit

Spyware, cavalo de Troia (trojan) e ransomware Cavalo de Troia (trojan), backdoor e ransomware

**Conferir resposta**

[Página anterior](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=7)

[Próxima página](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=13)

[Curso em Segurança da Informação](https://mooc-seginfo.appspot.com/moocseg/)

[williamdasilvamelo@gmail.com](mailto:williamdasilvamelo@gmail.com) | [Dashboard](https://mooc-seginfo.appspot.com/moocseg/dashboard) | Sair

[Notificações](https://mooc-seginfo.appspot.com/moocseg/announcements) [**Curso**](https://mooc-seginfo.appspot.com/moocseg/course)[Progresso](https://mooc-seginfo.appspot.com/moocseg/student/home)

**Search**

[Curso](https://mooc-seginfo.appspot.com/moocseg/course) › [Unidade 2](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1) › Lição 8

# Unidade 2 - Programas Maliciosos - Malware [](https://mooc-seginfo.appspot.com/moocseg/dashboard?action=edit_unit&amp;key=1)

 [2.1 Vírus](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=2)

 [2.2 Worms](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=3)



**Desafio Prático** 

Crie um arquivo de "vírus" com o nome "DOCUMENTO" que seja capaz de

desligar a máquina do usuário quando ele executar o arquivo.

 [2.3 Bot e Botnet](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=4)

 [2.4 Spyware](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=5)

 [2.5 Backdoor](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=6)

 [2.6 Cavalo de Tróia](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=7)

 [2.7](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

[Ransomware](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

 **2.8 Desafio Prático**

 [2.9 Tutorial Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=43)

[Página anterior](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

[Próxima página](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=43)

https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&lesson=13 1/1

### [Curso em Segurança da Informação](https://mooc-seginfo.appspot.com/moocseg/)

[williamdasilvamelo@gmail.com](mailto:williamdasilvamelo@gmail.com) | [Dashboard](https://mooc-seginfo.appspot.com/moocseg/dashboard) | Sair

[Notificações](https://mooc-seginfo.appspot.com/moocseg/announcements) [**Curso**](https://mooc-seginfo.appspot.com/moocseg/course)[Progresso](https://mooc-seginfo.appspot.com/moocseg/student/home)

**Search**

[Curso](https://mooc-seginfo.appspot.com/moocseg/course) › [Unidade 2](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1) › Lição 9

# Unidade 2 - Programas Maliciosos - Malware [](https://mooc-seginfo.appspot.com/moocseg/dashboard?action=edit_unit&amp;key=1)

 [2.1 Vírus](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=2)

 [2.2 Worms](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=3)

 [2.3 Bot e Botnet](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=4)

 [2.4 Spyware](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=5)

 [2.5 Backdoor](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=6)

 [2.6 Cavalo de Tróia](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=7)

 [2.7](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

[Ransomware](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=14)

 [2.8 Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=13)

 **2.9 Tutorial Desafio Prático**

##### Tutorial Desafio Prático 

Informações necessárias ao leitor:

**O que é o um arquivo .bat?**

Um arquivo .bat pode ser definido como um conjunto de comandos executados sequencialmente, criado para o MS-DOS, onde tem a função de automatizar tarefas rotineiras e muitas vezes trabalhosas.

**Como criar um arquivo .bat?**

Basta abrir o bloco de notas, e digitar os comandos pertinentes, após a sua conclusão, salve o arquivo com a extensão .bat (exemplo: nomedoarquivo.bat).

**Criação do arquivo:**

Abra o bloco de notas ou outro programa que salve arquivos com a extensão.txt.

Digite o comando “shutdown -t 3600 -s -f -c “Digite a mensagem"

**PARAMENTOS:**

**-t** = Define o tempo limite para desligamento em segundos, no exemplo 3600s = 1h.

**-s** = Desliga o computador.

**-f** = Força o encerramento da execução de aplicativos que estejam abertos.

**-c** = "COMENTÁRIOS ENTRE ASPAS" Comentário sobre

desligamento (máximo de 127 caracteres).

**Ex: shutdown -s -t 60 -c "Você tem 1 minuto para salvar o seu**

**Windows, boa sorte :D!"**

Escolha o local e salve o arquivo, Observação: Na hora do salvamento, coloque o nome e no final adicione “.bat”. Exemplo: “DOCUMENTO.bat” Pronto, o arquivo está completo. Após alguém executá-lo irá iniciar a contagem regressiva do tempo (caso tenha sido adicionado o parâmetro “t”) e o computador irá desligar ao fim. Um atacante enviaria esse arquivo por

email ou rede social.

[Página anterior](https://mooc-seginfo.appspot.com/moocseg/unit?unit=1&amp;lesson=13)

[Fim](https://mooc-seginfo.appspot.com/moocseg/course)

Estudo de caso - Malware

\*Obrigatório

Endereço de e-mail \*

Seu e-mail



Na quinta-feira de manhã, John, um empregado da universidade XYZ, notou uma mensagem de aviso em seu computador dizendo que o sistema foi atacado por um Win32.VB worm. Mesmo que o software antivírus estava presente no sistema, o software não conseguiu detectar o novo worm porque não foi atualizado para a versão mais recente.

Quando John tentou abrir seu e-mail, ele experimentou uma conexão de internet lenta. Ele percebeu que havia alguns nomes de arquivo incomuns no disco. John imediatamente informou seu amigo Bob, que também era um empregado XYZ, do problema. Bob checou seu computador em seu escritório e experimentou o mesmo problema que John. John e Bob verificado vários computadores nos laboratórios, e descobriu que Win32.VB verme havia infectado muitos outros computadores no laboratório. Eles contataram o setor de TI da Universidade XYZ. O administrador do sistema verificou os computadores constatando o incidente de segurança da informação. Como um resultado do ataque verme as atividades no laboratório da Universidade XYZ foram suspensas, o que causou um grande inconveniente. Na sua opinião, qual foi a vulnerabilidade explorada ? Quais medidas devem ser adotadas para conter e se recuperar do incidente de segurança da informação relatado no estudo de caso acima? \*

Sua resposta

Enviar

0 pontos

Nunca envie senhas pelo Formulários Google.

Este formulário foi criado em INSTITUTO FEDERAL DO PIAUÍ. D enunciar abuso

[Formulários](https://www.google.com/forms/about/?utm_source=product&amp;utm_medium=forms_logo&amp;utm_campaign=forms)

X



[Curso em Segurança da Informação](https://mooc-seginfo.appspot.com/moocseg/)

[williamdasilvamelo@gmail.com](mailto:williamdasilvamelo@gmail.com) | [Dashboard](https://mooc-seginfo.appspot.com/moocseg/dashboard) | Sair

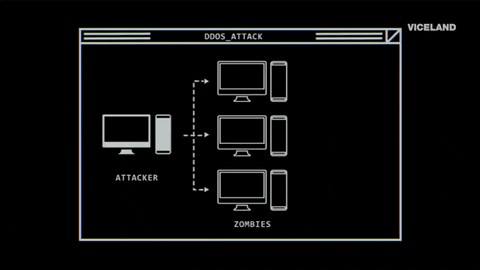
[Notificações](https://mooc-seginfo.appspot.com/moocseg/announcements) [**Curso**](https://mooc-seginfo.appspot.com/moocseg/course)[Progresso](https://mooc-seginfo.appspot.com/moocseg/student/home)

[Curso](https://mooc-seginfo.appspot.com/moocseg/course) › [Unidade 3](https://mooc-seginfo.appspot.com/moocseg/unit?unit=22)

**Search**

Unidade 3 - Golpes e ataques na Internet [□](https://mooc-seginfo.appspot.com/moocseg/dashboard?action=edit_unit&amp;key=22)

* 1. [Varredura em redes (Scan)](https://mooc-seginfo.appspot.com/moocseg/unit?unit=22&amp;lesson_title_28)



 [3.2 Falsificação de e- mail (E-mail spoofing)](https://mooc-seginfo.appspot.com/moocseg/unit?unit=22&amp;lesson_title_24)

 [3.3 Spam](https://mooc-seginfo.appspot.com/moocseg/unit?unit=22&amp;lesson_title_30)

 [3.4 Furto de identidade](https://mooc-seginfo.appspot.com/moocseg/unit?unit=22&amp;lesson_title_23)

 [3.5 Fraude de antecipação de recursos (Advance fee fraud)](https://mooc-seginfo.appspot.com/moocseg/unit?unit=22&amp;lesson_title_25)

 [3.6 Phishing](https://mooc-seginfo.appspot.com/moocseg/unit?unit=22&amp;lesson_title_26)

 [3.7 Golpes de comércio eletrônico](https://mooc-seginfo.appspot.com/moocseg/unit?unit=22&amp;lesson_title_27)

 [3.8 Interceptação de tráfego (Sniffing)](https://mooc-seginfo.appspot.com/moocseg/unit?unit=22&amp;lesson_title_29)

 [3.9 Força bruta (Brute force)](https://mooc-seginfo.appspot.com/moocseg/unit?unit=22&amp;lesson_title_31)

 [3.10 Desfiguração de página (Defacement)](https://mooc-seginfo.appspot.com/moocseg/unit?unit=22&amp;lesson_title_32)

 [3.11 Negação de serviço (DoS e DDoS)](https://mooc-seginfo.appspot.com/moocseg/unit?unit=22&amp;lesson_title_33)

 [3.12 Desafio Prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=22&amp;lesson_title_47)

 [3.13 Tutorial desafio prático](https://mooc-seginfo.appspot.com/moocseg/unit?unit=22&amp;lesson_title_38)

 [3.14 Trabalho em equipe](https://mooc-seginfo.appspot.com/moocseg/unit?unit=22&amp;lesson_title_44) (Private)

Ataques costumam ocorrer na Internet com diversos objetivos, visando diferentes alvos e usando variadas técnicas. Qualquer serviço, computador ou rede que seja acessível via Internet pode ser alvo de um ataque, assim como qualquer computador com acesso à Internet pode participar de um ataque.

Os motivos que levam os atacantes a desferir ataques na Internet são bastante diversos, variando da simples diversão até a realização de ações criminosas. Alguns exemplos são:

**Demonstração de poder:** mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente.

**Prestígio:** vangloriar-se, perante outros atacantes, por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar *sites* considerados visados ou difíceis de serem atacados; disputar com outros atacantes ou grupos de atacantes para revelar quem consegue realizar o maior número de ataques ou ser o primeiro a conseguir atingir um determinado alvo.

**Motivações financeiras:** coletar e utilizar informações confidenciais de usuários para aplicar golpes.

**Motivações ideológicas:** tornar inacessível ou invadir *sites* que divulguem conteúdo contrário à opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia.

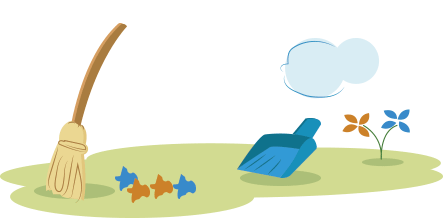
**Motivações comerciais:** tornar inacessível ou invadir *sites* e computadores de empresas concorrentes, para tentar impedir o acesso dos clientes ou comprometer a reputação destas empresas.

Normalmente, não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial e, por este motivo, golpistas vêm concentrando esforços na exploração de fragilidades dos usuários. Utilizando técnicas de engenharia social e por diferentes meios e discursos, os golpistas procuram enganar e persuadir os potenciais vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas.



**Varredura em redes (Scan)** □

Varredura em redes, ou scan[1](https://cartilha.cert.br/ataques/#footnote001), é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.



A varredura em redes e a exploração de vulnerabilidades associadas podem ser usadas de forma:

**Legítima**: por pessoas devidamente autorizadas, para verificar a segurança de computadores e redes e, assim, tomar medidas corretivas e preventivas.

**Maliciosa**: por atacantes, para explorar as vulnerabilidades encontradas nos serviços disponibilizados e nos programas instalados para a execução de atividades maliciosas. Os atacantes também podem utilizar os computadores ativos detectados como potenciais alvos no processo de propagação automática de códigos maliciosos e em ataques de força bruta.

* + 1. Não confunda scan com scam. Scams, com "m", são esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras.



**Falsificação de e-mail (E-mail spoofing)** □

Falsificação de *e-mail*, ou *e-mail spoofing*, é uma técnica que consiste em alterar campos do cabeçalho de um *e-mail*, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

Esta técnica é possível devido a características do protocolo SMTP (***S****imple* ***M****ail* ***T****ransfer* ***P****rotocol*) que permitem que campos do cabeçalho, como "From:" (endereço de quem enviou a mensagem), "Reply-To" (endereço de resposta da mensagem) e "Return-Path" (endereço para onde possíveis erros no envio da mensagem são reportados), sejam falsificados.

Ataques deste tipo são bastante usados para propagação de códigos maliciosos, envio de *spam* e em golpes de *phishing*. Atacantes utilizam-se de endereços de *e-mail* coletados de computadores infectados para enviar mensagens e tentar fazer com que os seus destinatários acreditem que elas partiram de pessoas conhecidas.

Exemplos de *e-mails* com campos falsificados são aqueles recebidos como sendo:



de alguém conhecido, solicitando que você clique em um *link* ou execute um arquivo anexo;

do seu banco, solicitando que você siga um *link* fornecido na própria mensagem e informe dados da sua conta bancária;

do administrador do serviço de *e-mail* que você utiliza, solicitando informações pessoais e ameaçando bloquear a sua conta caso você não as envie.

Você também pode já ter observado situações onde o seu próprio endereço de *e-mail* foi indevidamente utilizado.

Alguns indícios disto são:

você recebe respostas de *e-mails* que você nunca enviou;

você recebe *e-mails* aparentemente enviados por você mesmo, sem que você tenha feito isto;

você recebe mensagens de devolução de *e-mails* que você nunca enviou, reportando erros como usuário desconhecido e caixa de entrada lotada (cota excedida).

**Vulnerabilidades exploradas**

Campos do protocolo SMTP

Fragilidade de equipamento (Rever tópico 2.8 Vulnerabilidades x Prevenção) Contato utilizando engenharia social

Vários computadores de uma rede estão gerando spam, disseminando vírus, atacando computadores e servidores*Um ponto* de forma não prevista pelos administradores. Foi identificado um malware que é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados nos computadores infectados, tornando-os zumbis. Tal comportamento é tipicamente ocasionado por uma ação de

Adware Phishing Botnet Keylogger Spyware

**Conferir resposta**



**Spam** □

Spam[1](https://cartilha.cert.br/spam/#footnote001) 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.

Spams estão diretamente associados a ataques à segurança da Internet e do usuário, sendo um dos grandes responsáveis pela propagação de códigos maliciosos, disseminação de golpes e venda ilegal de produtos.

Algumas das formas como você pode ser afetado pelos problemas causados pelos spams são:

Perda de mensagens importantes: devido ao grande volume de spam recebido, você corre o risco de não ler mensagens importantes, lê-las com atraso ou apagá-las por engano.

Conteúdo impróprio ou ofensivo: como grande parte dos spams são enviados para conjuntos aleatórios de endereços de e-mail, é bastante provável que você receba mensagens cujo conteúdo considere impróprio ou ofensivo.

Gasto desnecessário de tempo: para cada spam recebido, é necessário que você

gaste um tempo para lê-lo, identificá-lo e removê-lo da sua caixa postal, o que pode resultar em gasto desnecessário de tempo e em perda de produtividade.

Não recebimento de e-mails: caso o número de spams recebidos seja grande e você utilize um serviço de e-mail que limite o tamanho de caixa postal, você corre o risco de lotar a sua área de e-mail e, até que consiga liberar espaço, ficará impedido de receber novas mensagens.

Classificação errada de mensagens: caso utilize sistemas de filtragem com regras antispam ineficientes, você corre o risco de ter mensagens legítimas classificadas como spam e que, de acordo com as suas configurações, podem ser apagadas, movidas para quarentena ou redirecionadas para outras pastas de e-mail.

Independente do tipo de acesso à Internet usado, é o destinatário do spam quem paga pelo envio da mensagem. Os provedores, para tentar minimizar os problemas, provisionam mais recursos computacionais e os custos derivados acabam sendo transferidos e incorporados ao valor mensal que os usuários pagam.

Alguns dos problemas relacionados a spam que provedores e empresas costumam enfrentar são:

Impacto na banda: o volume de tráfego gerado pelos spams faz com que seja necessário aumentar a capacidade dos links de conexão com a Internet.

Má utilização dos servidores: boa parte dos recursos dos servidores de e-mail, como tempo de processamento e espaço em disco, são consumidos no tratamento de mensagens não solicitadas.

Inclusão em listas de bloqueio: um provedor que tenha usuários envolvidos em casos de envio de spam pode ter a rede incluída em listas de bloqueio, o que pode prejudicar o envio de e-mails por parte dos demais usuários e resultar em perda de clientes.

Investimento extra em recursos: os problemas gerados pelos spams fazem com que seja necessário aumentar os investimentos, para a aquisição de equipamentos e sistemas de filtragem e para a contratação de mais técnicos especializados na sua operação.

Os spammers utilizam diversas técnicas para coletar endereços de e-mail, desde a compra de bancos de dados até a produção de suas próprias listas, geradas a partir de:

Ataques de dicionário: consistem em formar endereços de e-mail a partir de listas de nomes de pessoas, de palavras presentes em dicionários e/ou da combinação de caracteres alfanuméricos.

Códigos maliciosos: muitos códigos maliciosos são projetados para varrer o computador infectado em busca de endereços de e-mail que, posteriormente, são repassados para os spammers.

Harvesting: consiste em coletar endereços de e-mail por meio de varreduras em páginas Web e arquivos de listas de discussão, entre outros. Para tentar combater esta técnica, muitas páginas Web e listas de discussão apresentam os endereços de forma ofuscada (por exemplo, substituindo o "@" por "(at)" e os pontos pela palavra "dot"). Infelizmente, tais substituições são previstas por vários dos programas que implementam esta técnica.

Após efetuarem a coleta, os spammers procuram confirmar a existência dos ende costumam se utilizar de artifícios, como:

enviar mensagens para os endereços coletados e, com base nas respostas recebidas dos servidores de e-mail, identificar quais endereços são válidos e quais não são;

incluir no spam um suposto mecanismo para a remoção da lista de e-mails, como um link ou um endereço de e-mail (quando o usuário solicita a remoção, na verdade está confirmando para o spammer que aquele endereço de e-mail é válido e realmente utilizado);

incluir no spam uma imagem do tipo Web bug, projetada para monitorar o acesso a uma página Web ou e-mail (quando o usuário abre o spam, o Web bug é acessado e o spammer recebe a confirmação que aquele endereço de e-mail é válido).

1. Para mais detalhes acesse o site Antispam.br, <http://www.antispam.br/>, mantido pelo Comitê Gestor da Internet no Brasil (CGI.br), que constitui uma fonte de referência sobre o spam e tem o compromisso de informar usuários e administradores de redes sobre as implicações destas mensagens e as formas de proteção e de combate existentes. [voltar](https://cartilha.cert.br/spam/#sup_footnote001)

**Vulnerabilidades Exploradas**

Informações pessoais divulgadas na internet ou redes sociais Preencher cadastros de entidades duvidosas

Campos do protocolo SMTP Falsificação de email's

Contato via e-mail utilizando engenharia social

**Prevenção**

É muito importante que você saiba como identificar os spams, para poder detectá-los mais facilmente e agir adequadamente. As principais características[2](https://cartilha.cert.br/spam/#footnote002) dos spams são:

**Apresentam cabeçalho suspeito**: o cabeçalho do e-mail aparece incompleto, por exemplo, os campos de remetente e/ou destinatário aparecem vazios ou com apelidos/nomes genéricos, como "amigo@" e "suporte@".

**Apresentam no campo Assunto (Subject) palavras com grafia errada ou suspeita**: a maioria dos filtros antispam utiliza o conteúdo deste campo para barrar e-mails com assuntos considerados suspeitos. No entanto, os spammers adaptam-se e tentam enganar os filtros colocando neste campo conteúdos enganosos, como ``vi@gra'' (em vez de "viagra").

**Apresentam no campo Assunto textos alarmantes ou vagos**: na tentativa de confundir os filtros antispam e de atrair a atenção dos usuários, os spammers costumam colocar textos alarmantes, atraentes ou vagos demais, como "Sua senha está inválida", "A informação que você pediu" e "Parabéns".

**Oferecem opção de remoção da lista de divulgação**: alguns spams tentam justificar o abuso, alegando que é possível sair da lista de divulgação, clicando no endereço anexo ao e-mail. Este artifício, porém, além de não retirar o seu endereço de e-mail da lista, também serve para validar que ele realmente existe e que é lido por alguém.

**Prometem que serão enviados "uma única vez"**: ao alegarem isto, sugerem que não é necessário que você tome alguma ação para impedir que a mensagem seja novamente enviada.

**Baseiam-se em leis e regulamentações inexistentes**: muitos spams tentam embasar o envio em leis e regulamentações brasileiras referentes à prática de spam que, até o momento de escrita desta Cartilha, não existem.

Alguns cuidados que você deve tomar para tentar reduzir a quantidade de spams recebidos são:

procure filtrar as mensagens indesejadas, por meio de programas instalados em servidores ou em seu computador e de sistemas integrados a Webmails e leitores de e-mails. É interessante consultar o seu provedor de e-mail, ou o administrador de sua rede, para verificar os recursos existentes e como usá-los;

alguns Webmails usam filtros baseados em "tira-teima", onde é exigido do remetente a confirmação do envio (após confirmá-la, ele é incluído em uma lista de remetentes autorizados e, a partir daí, pode enviar e-mails livremente). Ao usar esses sistemas, procure autorizar previamente os remetentes desejáveis, incluindo fóruns e listas de discussão, pois nem todos confirmam o envio e, assim, você pode deixar de receber mensagens importantes;

muitos filtros colocam as mensagens classificadas como spam em quarentena. É importante que você, de tempos em tempos, verifique esta pasta, pois podem acontecer casos de falsos positivos e mensagens legítimas virem a ser classificadas como spam. Caso você, mesmo usando filtros, receba um spam, deve classificá-lo como tal, pois estará ajudando a treinar o filtro;

seja cuidadoso ao fornecer seu endereço de e-mail. Existem situações onde não há motivo para que o seu e- mail seja fornecido. Ao preencher um cadastro, por exemplo, pense se é realmente necessário fornecer o seu e- mail e se você deseja receber mensagens deste local;

fique atento a opções pré-selecionadas. Em alguns formulários ou cadastros preenchidos pela Internet, existe a pergunta se você quer receber e-mails, por exemplo, sobre promoções e lançamentos de produtos, cuja resposta já vem marcada como afirmativa. Fique atento a esta questão e desmarque-a, caso não deseje receber este tipo de mensagem;

não siga links recebidos em spams e não responda mensagens deste tipo (estas ações podem servir para confirmar que seu e-mail é válido);

desabilite a abertura de imagens em e-mails HTML (o fato de uma imagem ser acessada pode servir para confirmar que a mensagem foi lida);

crie contas de e-mail secundárias e forneça-as em locais onde as chances de receber spam são grandes, como ao preencher cadastros em lojas e em listas de discussão;

utilize as opções de privacidade das redes sociais (algumas redes permitem esconder o seu endereço de e-mail ou restringir as pessoas que terão acesso a ele);

respeite o endereço de e-mail de outras pessoas. Use a opção de "Bcc:" ao enviar e-mail para grandes quantidades de pessoas. Ao encaminhar mensagens, apague a lista de antigos destinatários, pois mensagens reencaminhadas podem servir como fonte de coleta para spammers.

1. Vale ressaltar que nem todas essas características podem estar presentes ao mesmo tempo, em um mesmo spam. Da mesma forma, podem existir spams que não atendam às propriedades citadas, podendo, eventualmente, ser um novo tipo.

Furto 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.

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 maliciosos ataques de força bruta e interceptação de tráfego.

Caso a sua identidade seja furtada, você poderá arcar com consequências como perdas financeiras, perda de reputação e falta de crédito. Além disto, pode levar muito tempo e ser bastante desgastante até que você consiga reverter todos os problemas causados pelo impostor.

**Vulnerabilidades**

Disponibilizar dados pessoais de forma pública na internet Utilização de senhas fracas ou óbvias

Compartilhar localização geográfica, rotina, gostos, preferências em redes sociais Armazenar arquivos, documentos e dados pessoais sem criptografia

Preencher cadastros de entidades duvidosas

Deixar computador ou outro dispositivo sujeito a código malicioso

**Prevenção**

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. 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.

**Cuidados a serem tomados ao usar suas contas e senhas:**

certifique-se de não estar sendo observado ao digitar as suas senhas; não forneça as suas senhas para outra pessoa, em hipótese alguma;

certifique-se de fechar a sua sessão ao acessar sites que requeiram o uso de senhas. Use a opção de sair (logout), pois isto evita que suas informações sejam mantidas no navegador;

elabore senhas boas (uma senha boa, bem elaborada, é aquela que é difícil de ser descoberta (forte) e fácil de ser lembrada. Não convém que você crie uma senha forte se, quando for usá-la, não conseguir

recordá-la. Também não convém que você crie uma senha fácil de ser lembrada se ela puder ser facilmente descoberta por um atacante.)

**Não utilize em suas senhas:**

**Qualquer tipo de dado pessoal**: evite nomes, sobrenomes, contas de usuário, números de documentos, placas de carros, números de telefones e datas

**Sequências de teclado**: evite senhas associadas à proximidade entre os caracteres no teclado

**Palavras que façam parte de listas**: evite palavras presentes em listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes, dicionários de diferentes idiomas, etc

É necessário também que você fique atento a alguns indícios que podem demonstrar que su’a 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.

Fraude de antecipação de recursos (Advance fee fraud) □



A fraude de antecipação de recursos, ou *advance fee fraud*, é aquela na qual um golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício.

Por meio do recebimento de mensagens eletrônicas ou do acesso a *sites* fraudulentos, a pessoa é envolvida em alguma situação ou história mirabolante, que justifique a necessidade de envio de informações pessoais ou a realização de algum pagamento adiantado, para a obtenção de um benefício futuro. Após fornecer os recursos solicitados a pessoa percebe que o tal benefício prometido não existe, constata que foi vítima de um golpe e que seus dados/dinheiro estão em posse de golpistas.

O Golpe da Nigéria (*Nigerian 4-1-9 Scam***1**) é um dos tipos de fraude de antecipação de recursos mais conhecidos e é aplicado, geralmente, da seguinte forma:

1. Você recebe uma mensagem eletrônica em nome de alguém ou de alguma instituição dizendo-se ser da Nigéria, na qual é solicitado que você atue como intermediário em uma transferência internacional de fundos;

2. o valor citado na mensagem é absurdamente alto e, caso você aceite intermediar a transação, recebe a promessa de futuramente ser recompensado com uma porcentagem deste valor;

3. o motivo, descrito na mensagem, pelo qual você foi selecionado para participar da transação geralmente é a indicação de algum funcionário ou amigo que o apontou como sendo uma pessoa honesta, confiável e merecedora do tal benefício;

4. a mensagem deixa claro que se trata de uma transferência ilegal e, por isto, solicita sigilo absoluto e urgência na resposta, caso contrário, a pessoa procurará por outro parceiro e você perderá a oportunidade;

5. após responder a mensagem e aceitar a proposta, os golpistas solicitam que você pague antecipadamente uma quantia bem elevada (porém bem inferior ao total que lhe foi prometido) para arcar com custos, como

advogados e taxas de transferência de fundos;

6. após informar os dados e efetivar o pagamento solicitado, você é informado que necessita realizar novos pagamentos ou perde o contato com os golpistas;

finalmente, você percebe que, além de perder todo o dinheiro investido, nunca verá a quantia prometida como recompensa e que seus dados podem estar sendo indevidamente usados.

Apesar deste golpe ter ficado conhecido como sendo da Nigéria, já foram registrados diversos casos semelhantes, originados ou que mencionavam outros países, geralmente de regiões pobres ou que estejam passando por conflitos políticos, econômicos ou raciais.

A fraude de antecipação de recursos possui diversas variações que, apesar de apresentarem diferentes discursos, assemelham-se pela forma como são aplicadas e pelos danos causados. Algumas destas variações são:

**Loteria internacional:** você recebe um *e-mail* informando que foi sorteado em uma loteria internacional, mas que para receber o prêmio a que tem direito, precisa fornecer seus dados pessoais e informações sobre a sua conta bancária.

**Crédito fácil:** você recebe um *e-mail* contendo uma oferta de empréstimo ou financiamento com taxas de juros muito inferiores às praticadas no mercado. Após o seu crédito ser supostamente aprovado você é informado que necessita efetuar um depósito bancário para o ressarcimento das despesas.

**Doação de animais:** você deseja adquirir um animal de uma raça bastante cara e, ao pesquisar por possíveis vendedores, descobre que há *sites* oferecendo estes animais para doação. Após entrar em contato, é solicitado que você envie dinheiro para despesas de transporte.

**Oferta de emprego:** você recebe uma mensagem em seu celular contendo uma proposta tentadora de emprego. Para efetivar a contratação, no entanto, é necessário que você informe detalhes de sua conta bancária.

**Noiva russa:** alguém deixa um recado em sua rede social contendo insinuações sobre um possível relacionamento amoroso entre vocês. Esta pessoa mora em outro país, geralmente a Rússia, e após alguns contatos iniciais sugere que vocês se encontrem pessoalmente, mas, para que ela possa vir até o seu país, necessita ajuda financeira para as despesas de viagem.

**Vulnerabilidade explorada**

Falta de conhecimento sobre engenharia social

**Prevenção:**

A melhor forma de se prevenir é identificar as mensagens contendo tentativas de golpes. Uma mensagem deste tipo, geralmente, possui características como:

oferece quantias astronômicas de dinheiro; solicita sigilo nas transações;

solicita que você a responda rapidamente;

apresenta palavras como "urgente" e "confidencial" no campo de assunto;

apresenta erros gramaticais e de ortografia (muitas mensagens são escritas por meio do uso de programas tradutores e podem apresentar erros de tradução e de concordância).

Além disto, adotar uma postura preventiva pode, muitas vezes, evitar que você seja vítima de golpes. Por isto, é muito importante que você:

questione-se por que justamente você, entre os inúmeros usuários da Internet, foi escolhido para receber o benefício proposto na mensagem e como chegaram até você;

desconfie de situações onde é necessário efetuar algum pagamento com a promessa de futuramente receber um valor maior (pense que, em muitos casos, as despesas poderiam ser descontadas do valor total).

Aplicar a sabedoria popular de ditados como "Quando a esmola é demais, o santo desconfia" ou "Tudo que vem fácil, vai fácil", também pode ajudá-lo nesses casos.

Vale alertar que mensagens deste tipo nunca devem ser respondidas, pois isto pode servir para confirmar que o seu endereço de *e-mail* é válido. Esta informação pode ser usada, por exemplo, para incluí-lo em listas de *spam* ou de possíveis vítimas em outros tipos de golpes.



E-mail spoofing é uma técnica que pode ser utilizada para propagação de códigos maliciosos, envio de spam e *Um ponto*

golpes de phishing. Esta técnica consiste em:

Alterar os campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

Alterar os campos do protocolo SMTP, de forma que os e-mails do usuário sejam direcionados para outra sem que ele saiba.

falsificar o protocolo SMTP para inspecionar os dados trafegados na caixa de e-mail do usuário, por meio do uso de programas específicos.

Efetuar buscas minuciosas no computador do usuário, com o objetivo de identificar informações sigilosas.

alterar as configurações de um servidor de e-mail para que dispare uma infinidade de e-mails falsos até encher a caixa de correio de um ou muitos usuários

**Conferir resposta**

Phishing □

*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, como exemplificado na Tabela abaixo. Exemplos de situações envolvendo *phishing* são:

**Páginas ou sites falsos 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 ou sites falsos 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.

**Vulnerabilidades Exploradas**

Informações pessoais divulgadas na internet ou redes sociais Acessar links duvidosos e desconhecidos

Acessar banners promocionais por meio de sites duvidosos e desconhecidos Disponibilizar dados pessoais de forma pública na internet

Falsificação de email's

Falta de conhecimento sobre engenharia social

|  |  |
| --- | --- |
| Álbuns de fotos e vídeos | pessoa supostamente conhecida, celebridades algum fato noticiado em jornais, revistas ou televisão traição, nudez ou pornografia, serviço de acompanhantes |
| Antivírus | atualização de vacinas, eliminação de vírus lançamento de nova versão ou de novas funcionalidades |
| Associações assistenciais | AACD Teleton, Click Fome, Criança Esperança |
| Avisos judiciais | intimação para participação em audiência comunicado de protesto, ordem de despejo |
| Cartões de crédito | programa de fidelidade, promoção |
| Cartões virtuais | UOL, *Voxcards*, Yahoo! Cartões, O Carteiro, *Emotioncard* |
| Comércio eletrônico | cobrança de débitos, confirmação de compra atualização de cadastro, devolução de produtos oferta em *site* de compras coletivas |
| Companhias aéreas | promoção, programa de milhagem |
| Eleições | título eleitoral cancelado, convocação para mesário |
| Empregos | cadastro e atualização de currículos, processo seletivo em aberto |
| Imposto de renda | nova versão ou correção de programa consulta de restituição, problema nos dados da declaração |
| *Internet Banking* | unificação de bancos e contas, suspensão de acesso atualização de cadastro e de cartão de senhas lançamento ou atualização de módulo de segurança comprovante de transferência e depósito, cadastramento de computador |
| Multas e infrações de trânsito | aviso de recebimento, recurso, transferência de pontos |
| Músicas | canção dedicada por amigos |
|  |  |

|  |  |
| --- | --- |
| Notícias e  boatos | fato amplamente noticiado, ataque terrorista, tragédia natural |
| Prêmios | loteria, instituição financeira |
| Programas em geral | lançamento de nova versão ou de novas funcionalidades |
| Promoções | vale-compra, assinatura de jornal e revista desconto elevado, preço muito reduzido, distribuição gratuita |
| Propagandas | produto, curso, treinamento, concurso |
| *Reality shows* | Big Brother Brasil, A Fazenda, Ídolos |
| Redes sociais | notificação pendente, convite para participação aviso sobre foto marcada, permissão para divulgação de foto |
| Serviços de Correios | recebimento de telegrama *online* |
| Serviços de *e- mail* | recadastramento, caixa postal lotada, atualização de banco de dados |
| Serviços de proteção de crédito | regularização de débitos, restrição ou pendência financeira |
| Serviços de telefonia | recebimento de mensagem, pendência de débito bloqueio de serviços, detalhamento de fatura, créditos gratuitos |
| *Sites* com dicas de segurança | aviso de conta de *e-mail* sendo usada para envio de *spam* (Antispam.br) cartilha de segurança (CERT.br, FEBRABAN, Abranet, etc.) |
| Solicitações | orçamento, documento, relatório, cotação de preços, lista de produtos |

**Prevenção:**

fique atento a mensagens, recebidas em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em *links*;

questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens, como se houvesse alguma relação prévia entre vocês (por exemplo, se você não tem conta em um determinado banco, não há porque recadastrar dados ou atualizar módulos de segurança);

fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos;

não considere que uma mensagem é confiável com base na confiança que você deposita em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada

seja cuidadoso ao acessar *links*. Procure digitar o endereço diretamente no navegador *Web*;

verifique o *link* apresentado na mensagem. Golpistas costumam usar técnicas para ofuscar o *link* real para o *phishing***. Ao posicionar o *mouse* sobre o *link*, muitas vezes é possível ver o endereço real da página falsa ou código malicioso;**

utilize mecanismos de segurança, como programas *antimalware*, *firewall* pessoal e filtros *antiphishing*;

verifique se a página utiliza **conexão segura HTTP’s**. *Sites* de comércio eletrônico ou *Internet Banking*

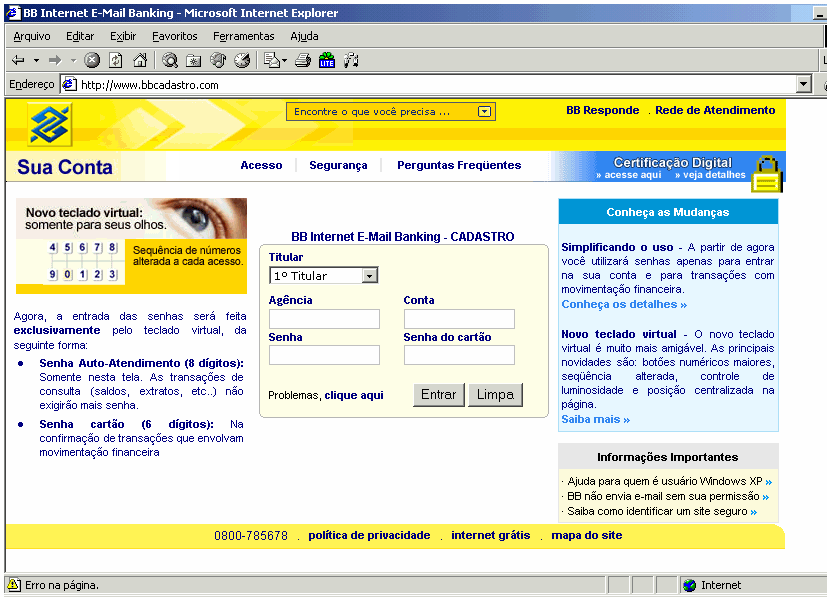
confiáveis sempre utilizam conexões seguras quando dados sensíveis são solicitados

verifique as informações mostradas no certificado. Caso a página falsa utilize conexão segura, um novo certificado será apresentado e, possivelmente, o endereço mostrado no navegador *Web* será diferente do endereço correspondente ao *site* verdadeiro ;

acesse a página da instituição que supostamente enviou a mensagem e procure por informações (você vai observar que não faz parte da política da maioria das empresas o envio de mensagens, de forma indiscriminada, para os seus usuários).

Abaixo alguns exemplos de páginas falsas de bancos capturadas na internet depois de ter recebido e-mails que convidavam a acessar tais páginas.

É importante ressaltar que, apesar dos bancos em geral tomarem todas a medidas possíveis para prevenir fraudes, nada impede que golpistas criem sites parecidos com os verdadeiros dos banco e os coloquem on-line em endereços diferentes, tentando depois enganar suas vítimas de várias maneiras para fazer com que acessem estes falsos site. Os bancos fazem tudo o possível para tentar tirar do ar estes falsos sites assim que tomarem conhecimento da existência deles, mas é responsabilidade dos usuários não acessá-los e verificar bem os sites que são acessados e sobretudo seguir SEMPRE as medidas de segurança indicadas pelos próprios bancos. Os modernos sistemas de internet banking dos bancos brasileiro, em geral, podem ser considerados plenamente seguros quando o usuário seguir sistematicamente e rigorosamente as indicações e procedimentos de segurança.



Abaixo alguns exemplos de páginas falsas (phishing) que utilizam e-mails assediar os usuários.

É importante ressaltar que, apesar dos bancos em geral tomarem todas as medidas possíveis para prevenir fraudes, nada impede que golpistas criem sites parecidos com os verdadeiros dos banco e os coloquem on-line em endereços diferentes, tentando depois enganar suas vítimas de várias maneiras para fazer com que acessem estes falsos sites. Os modernos sistemas de internet banking dos bancos, em geral, podem ser considerados plenamente seguros quando o usuário segue sistemática e rigorosamente as indicações e procedimentos de segurança.



**Golpes de comércio eletrônico** □



Golpes de comércio eletrônico são aqueles nos quais golpistas, com o objetivo de obter vantagens financeiras, exploram a relação de confiança existente entre as partes envolvidas em uma transação comercial.

**Vulnerabilidades Explodas**

Acessar links duvidosos e desconhecidos

Acessar banners promocionais por meio de sites duvidosos e desconhecidos Disponibilizar dados pessoais de forma pública na internet

Compartilhar localização geográfica, rotina, gostos, preferências em redes sociais Preencher cadastros de entidades duvidosas

Deixar computador ou outro dispositivo sujeito a código malicioso

**Golpe do site de comércio eletrônico fraudulento**

Neste golpe, o golpista cria um site fraudulento, com o objetivo específico de enganar os possíveis clientes que, após efetuarem os pagamentos, não recebem as mercadorias.

Para aumentar as chances de sucesso, o golpista costuma utilizar artifícios como: enviar spam, fazer propaganda via links patrocinados, anunciar descontos em sites de compras coletivas e ofertar produtos muito procurados e com preços abaixo dos praticados pelo mercado.

Além do comprador, que paga, mas não recebe a mercadoria, este tipo de golpe pode ter outras vítimas, como: uma empresa séria, cujo nome tenha sido vinculado ao golpe;

um site de compras coletivas, caso ele tenha intermediado a compra;

uma pessoa, cuja identidade tenha sido usada para a criação do site ou para abertura de empresas fantasmas.

**Prevenção:**

faça uma pesquisa de mercado, comparando o preço do produto exposto no site com os valores obtidos na pesquisa e desconfie caso ele seja muito abaixo dos praticados pelo mercado;

pesquise na Internet sobre o site, antes de efetuar a compra, para ver a opinião de outros clientes;

acesse sites especializados em tratar reclamações de consumidores insatisfeitos, para verificar se há reclamações referentes a esta empresa;

fique atento a propagandas recebidas através de spam (mais detalhes na lição Spam); seja cuidadoso ao acessar links patrocinados;

procure validar os dados de cadastro da empresa no site da Receita Federal;

não informe dados de pagamento caso o site não ofereça conexão segura ou não apresente um certificado confiável

**Golpe envolvendo sites de compras coletivas**

Sites de compras coletivas têm sido muito usados em golpes de sites de comércio eletrônico fraudulentos, como descrito anteriormente. Além dos riscos inerentes às relações comerciais cotidianas, os sites de compras coletivas também apresentam riscos próprios, gerados principalmente pela pressão imposta ao consumidor em tomar decisões rápidas pois, caso contrário, podem perder a oportunidade de compra.

Golpistas criam sites fraudulentos e os utilizam para anunciar produtos nos sites de compras coletivas e, assim, conseguir grande quantidade de vítimas em um curto intervalo de tempo.

Além disto, sites de compras coletivas também podem ser usados como tema de mensagens de phishing. Golpistas costumam mandar mensagens como se tivessem sido enviadas pelo site verdadeiro e, desta forma, tentam induzir o usuário a acessar uma página falsa e a fornecer dados pessoais, como número de cartão de crédito e senhas.

**Prevenção:**

procure não comprar por impulso apenas para garantir o produto ofertado;

seja cauteloso e faça pesquisas prévias, pois há casos de produtos anunciados com desconto, mas que na verdade, apresentam valores superiores aos de mercado;

pesquise na Internet sobre o site de compras coletivas, antes de efetuar a compra, para ver a opinião de outros clientes e observar se foi satisfatória a forma como os possíveis problemas foram resolvidos;

siga as dicas apresentadas na lição phishing para se prevenir contra esses golpes siga as dicas apresentadas na lição Golpe do site de comércio eletrônico fraudulento para se prevenir contra esses golpes

**Golpe do site de leilão e venda de produtos**

O golpe do site de leilão e venda de produtos é aquele, por meio do qual, um comprador ou vendedor age de má-fé e não cumpre com as obrigações acordadas ou utiliza os dados pessoais e financeiros envolvidos na transação comercial para outros fins. Por exemplo:

o comprador tenta receber a mercadoria sem realizar o pagamento ou o realiza por meio de transferência efetuada de uma conta bancária ilegítima ou furtada;

o vendedor tenta receber o pagamento sem efetuar a entrega da mercadoria ou a entrega danificada, falsificada, com características diferentes do anunciado ou adquirida de forma ilícita e criminosa (por exemplo, proveniente de contrabando ou de roubo de carga);

o comprador ou o vendedor envia e-mails falsos, em nome do sistema de gerenciamento de pagamentos, como forma de comprovar a realização do pagamento ou o envio da mercadoria que, na realidade, não foi feito.

**Pagamento de Boletos bancários**

Hoje em dia uma das maneiras mais usadas para pagamento é o boleto bancário. Você pode pagar a compra à vista e não precisa ter cartão de crédito para realizar a compra. Justamente, pelo aumento de pagamentos com boletos, as fraudes ou golpes do boleto também têm aumentado bastante.

É importante verificar atentamente o boleto bancário antes de realizar o pagamento. A dica principal é ver se o boleto está com padrão esquisito ou se tem erros de português. Se achar que está estranho não pague, teste as dicas seguintes.

Isso é feito para obrigar a pessoa a digitar o número do código do boleto no momento do pagamento e assim conseguir passar o boleto falso.

Outra dica é verificar as informações impressas como banco cedente, agência do beneficiário e código do banco. Estas informações sempre vêm escritas nos boletos autênticos. Cada Banco tem um número específico [que é o seu código de identificação, você pode conferir os números dos bancos na página da FEBRABAN ou do Banco Central.](http://www.bcb.gov.br/pom/spb/estatistica/port/ASTR003.pdf)

O exemplo abaixo mostra um boleto da Americanas emitido pelo Banco do Brasil. No canto superior esquerdo aparecem o nome e logo da instituição bancária. No código de barras, os três primeiros números são referentes ao código do banco emissor. Na foto abaixo é do Banco do Brasil que é 001. Preste atenção também nas informações do Beneficiário/Cedente se são realmente do local que está comprando. Todos documentos de cobrança de débitos devem conter nome, endereço e o número de inscrição no CPF ou CNPJ do fornecedor.

O código do beneficiário (antigo código do cedente) é o registro do beneficiário junto ao banco que emitiu o boleto. O da Americanas como mostrado acima é 15300-1, se procurar este número na internet vai achar várias informações sobre Americanas, Submarino, Shoptime, todas lojas do mesmo grupo.

O “Nosso número” é um código único gerado pelo banco para identificar este boleto que você vai pagar. Cada boleto gerado terá um ‘Nosso Número’ diferente. Portanto este campo não pode estar em branco.

Se mesmo depois de verificar todos os dados e ainda achar que o boleto é falso, não pague! Antes de fazer o pagamento entre em contato direto com a empresa que emitiu o boleto ou com o banco responsável. Não ligue para números de telefone impressos no boleto. Procure pelo número da loja ou do serviço na internet ou na lista telefônica! Os telefones que aparecerem no boleto podem te fazer ligar direto para os golpistas.

**O que fazer em caso de pagamento de boleto falso?**

[Se você já pagou o boleto falso não se desespere. De acordo com o artigo 20 do Código de Defesa do Consumidor o fornecedor de serviços deve responder pela reparação de danos causados ao consumidor. Como](http://www.planalto.gov.br/ccivil_03/leis/L8078.htm) o boleto é gerado por um banco e você está comprando de um fornecedor, os dois devem arcar com os prejuízos, pois eles que têm os dados que permitiram a confecção do boleto falso.

Para formalizar a denúncia do roubo, faça uma cópia do boleto falso e do comprovante do pagamento. Compareça a uma delegacia de polícia para registrar um boletim de ocorrência (BO). Com o BO em mãos procure o banco e a loja/fornecedor do serviço e registre a reclamação, tente solucionar o problema [amigavelmente. Se a empresa / fornecedor do serviço não resolver, procure um dos postos do Procon na sua cidade para registrar o ocorrido, o Procon tentará resolver o problema com você. Dependendo do fornecedor do](http://www.portaldoconsumidor.gov.br/procon.asp?acao=buscar) serviço também é possível fazer reclamação [pelo site Consumidor do Ministério da Justiça](https://www.consumidor.gov.br/).

Caso o Procon não resolva, você pode entrar com uma ação no Juizado Especial Cível para reembolso do valor. Também pode pedir indenização por danos morais ou materiais, se houver interrupção do serviço, negativação ou algum outro dano por causa do boleto falso. Lembrando que não é necessário advogado caso o prejuízo seja de até 20 salários mínimos, você mesmo pode entrar com a ação.

**Como se prevenir contra golpe do boleto na web?**

Se você costuma fazer muitas compras na internet é importante ter um antivírus atualizado instalado no computador. Alguns vírus são capazes de modificar o código do boleto quando você clicar na opção para gerar boleto. Não faça compras usando computadores públicos ou redes wi-fi abertas, golpistas podem interceptar a informação e fazer você gerar um boleto fraudado.

Sempre que receber algum email de cobrança com boleto anexado entre em contato direto com a empresa para confirmar. Não ligue para o telefone especificado no email! Procure na internet ou na lista telefônica pelo número oficial da empresa, pois o telefone no email pode estar alterado para o número dos golpistas. Caso tenha algum link no email copie e cole o endereço no site Virus Total <https://www.virustotal.com/#url> para analisar. Nunca clique em links sem ter certeza que é mesmo da empresa que enviou, pois a página que abrir pode conter vírus.

Se for fazer compras na web, sempre preste atenção no endereço que aparece na barra de endereço e se a loja está com o cadeado (https) no momento que for realizar o pagamento. O cadeado indica que a loja tem identidade confirmada, que a compra é segura e seus dados estão protegidos.

Essas são algumas dicas para identificar boleto falso antes de realizar o pagamento. Não dê bobeira! Se achar o boleto estranho não pague, confirme os dados com o fornecedor do serviço e com o banco emissor.

**Prevenção:**



faça uma pesquisa de mercado, comparando o preço do produto com os valores obtidos na pesquisa e desconfie caso ele seja muito abaixo dos praticados pelo mercado;

marque encontros em locais públicos caso a entrega dos produtos seja feita pessoalmente;

acesse sites especializados em tratar reclamações de consumidores insatisfeitos e que os coloca em contato com os responsáveis pela venda (você pode avaliar se a forma como o problema foi resolvido foi satisfatória ou não);

utilize sistemas de gerenciamento de pagamentos pois, além de dificultarem a aplicação dos golpes, impedem que seus dados pessoais e financeiros sejam enviados aos golpistas;

procure confirmar a realização de um pagamento diretamente em sua conta bancária ou pelo site do sistema de gerenciamento de pagamentos (não confie apenas em e-mails recebidos, pois eles podem ser falsos);

verifique a reputação do [usuário5](https://cartilha.cert.br/golpes/#footnote005) (muitos sites possuem sistemas que medem a reputação de compradores e vendedores, por meio da opinião de pessoas que já negociaram com este usuário);

acesse os sites, tanto do sistema de gerenciamento de pagamentos como o responsável pelas vendas, diretamente do navegador, sem clicar em links recebidos em mensagens;

mesmo que o vendedor lhe envie o código de rastreamento fornecido pelos Correios, não utilize esta informação para comprovar o envio e liberar o pagamento (até que você tenha a mercadoria em mãos não há nenhuma garantia de que o que foi enviado é realmente o que foi solicitado).

Spam e Spyware são basicamente:

*Um ponto*

Dois softwares do typo player de vídeo

Respectivamente, um programa espião e um e-mail não solicitado Respectivamente, um e-mail espião e um vírus de computador.

Dois tipos de vírus fatais que podem danificar um computador.

Respectivamente, um e-mail não solicitado e um programa espião.

**Conferir resposta**

**Interceptação de tráfego (Sniffing)** □

Interceptação de tráfego, ou sniffing, é uma técnica que consiste em inspecionar os dados trafegados em redes

de computadores, por meio do uso de programas específicos chamados de sniffers. Esta técnica pode ser utilizada de forma:

**Legítima**: por administradores de redes, para detectar problemas, analisar desempenho e monitorar atividades maliciosas relativas aos computadores ou redes por eles administrados.

**Maliciosa**: por atacantes, para capturar informações sensíveis, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.

Note que as informações capturadas por esta técnica são armazenadas na forma como trafegam, ou seja, informações que trafegam criptografadas apenas serão úteis ao atacante se ele conseguir decodificá-las

Força bruta (Brute force) □

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.

acesso físico a eles.

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

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.

**Negação de serviço (DoS e DDoS)** □

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. Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (Distributed Denial of Service).

O objetivo destes ataques não é invadir e nem coletar informações, mas sim exaurir recursos e causar indisponibilidades ao alvo. Quando isto ocorre, todas as pessoas que dependem dos recursos afetados são prejudicadas, pois ficam impossibilitadas de acessar ou realizar as operações desejadas.



**Desfiguração de página (Defacement)** □

Desfiguração de página, defacement ou pichação, é uma técnica que consiste em alterar o conteúdo da página Web de um site.

As principais formas que um atacante, neste caso também chamado de defacer, pode utilizar para desfigurar uma página Web são:

explorar erros da aplicação Web;

explorar vulnerabilidades do servidor de aplicação Web;

explorar vulnerabilidades da linguagem de programação ou dos pacotes utilizados no desenvolvimento da aplicação Web;

invadir o servidor onde a aplicação Web está hospedada e alterar diretamente os arquivos que compõem o site; furtar senhas de acesso à interface Web usada para administração remota.

Para ganhar mais visibilidade, chamar mais atenção e atingir maior número de visitantes, geralmente, os atacantes alteram a página principal do site, porém páginas internas também podem ser alteradas.

Utiliza um ou mais computadores para tornar indisponível um serviço provido.

Altera campos do cabeçalho de mensagens de e-mail para falsificar a origem da mensagem Captura e inspeciona dados que trafegam em uma rede

Altera o conteúdo de páginas web de forma maliciosa e publica informações contra a instituição mantenedora da página web.

Tenta adivinhar por tentativa e erro a senha de um usuário.

*Um ponto*

A técnica de Sniffing

**Conferir resposta**

Nos casos já registrados de ataques, os alvos ficaram impedidos de oferecer serviços durante o período em que eles ocorreram, mas, ao final, voltaram a operar normalmente, sem que tivesse havido vazamento de informações ou comprometimento de sistemas ou computadores.



**Conferir resposta**

Uma pessoa pode voluntariamente usar ferramentas e fazer com que seu computador seja utilizado em ataques. A grande maioria dos computadores, porém, participa dos ataques sem o conhecimento de seu dono, por estar infectado e fazendo parte de botnets (mais detalhes na lição bots e botnets da unidade programas maliciosos).

Ataques de negação de serviço podem ser realizados por diversos meios, como:

pelo envio de grande quantidade de requisições para um serviço, consumindo os recursos necessários ao seu funcionamento (processamento, número de conexões simultâneas, memória e espaço em disco, por exemplo) e impedindo que as requisições dos demais usuários sejam atendidas;

pela geração de grande tráfego de dados para uma rede, ocupando toda a banda disponível e tornando indisponível qualquer acesso a computadores ou serviços desta rede;

pela exploração de vulnerabilidades existentes em programas, que podem fazer com que um determinado serviço fique inacessível.

Nas situações onde há saturação de recursos, caso um serviço não tenha sido bem dimensionado, ele pode ficar inoperante ao tentar atender as próprias solicitações legítimas. Por exemplo, um site de transmissão dos jogos da Copa de Mundo pode não suportar uma grande quantidade de usuários que queiram assistir aos jogos finais e parar de funcionar.

Das alternativas a seguir, assinale a única que contém eventos que caracterizam uma tentativa de ataque do tipo *Um ponto*

força bruta.

A captura de dados sensíveis a partir de um programa espião instalado no computador do usuário. A operação local e não autorizada de estações ou servidores

Sobrecarga de servidores, alcançada por meio de ataques simultâneos e descentralizados Brechas resultantes de bugs no sistema

A repetição automática de tentativas de acesso a um recurso protegido, com senhas criadas a partir de combinações aleaórias ou extraídas de listas pré-definidas.



**Desafio Prático** □



Considerando as estratégias de golpe e ataques que ocorrem na internet, faça a cópia de uma página que contenha uma oferta real em um site de vendas conhecido como: magazine Luíza, Americanas, Ricardo eletro ou outro...

Tutorial desafio prático □



Considerando as estratégias de golpe e ataques que ocorrem na internet, faça a cópia de uma página que contenha uma oferta real em um site de vendas conhecido como: magazine Luíza, Americanas, Ricardo eletro ou outro...

Para tal, você poderá utilizar o software HTTRACK, faça o download a partir do link <https://www.httrack.com/page/2/>e escolha a versão compatível com seu sistema operacional. Execute o arquivo httrack .exe para instalar o programa e avance conforme modo de instalação padrão. A figura abaixo mostra a aparência da página inicial do programa instalado.

Para copiar um site clique em avançar, defina um nome para o projeto, escolha uma categoria (opcional) e defina o local onde os arquivos serão armazenados (ex. C/:Meus Sites).

Escolha a opção copiar site também existem outras opções como: receber arquivos específicos ou copiar todas as páginas do site. Porém, a opção copiar site será suficiente para copiar o anúncio.

Depois que você escolher a opção avançar será exibida uma nova tela que irá questionar ações a serem realizadas após o download, pode deixar marcadas as opções padrão, conforme ilusta a imagem abaixo.

Clicando em avançar o HTTRACK irá realizar o download dos arquivos, conforme mostra a figura abaixo, nesse exemplo eles estão armazenados em C:/Meus Sites

Depois da confirmação do download, acesse a pasta C:/Meus Sites, procure pelo nome do projeto criado e

selecionem o arquivo index.

Ao abrir o arquivo será exibido no navegador a página do anúncio, porém, ele estará armazenado no seu computador. Para um golpista bastaria alterar as algumas configurações relativas a emissão do boleto bancário para que, sua conta pessoal fosse a beneficiária. Posteriormente, hospedaria esse site copiado em outro

domínio e encaminharia as ofertas via email ou com publicações em redes sociais.

**Trabalho em equipe (Private)** □

Nem todos devem visualizar

Estudo de caso - Golpe de comércio eletrônico

\*Obrigatório

Endereço de e-mail \*

Seu e-mail



Você está acessando uma rede social logado em sua conta pessoal e de repente visualiza um anúncio do site americanas contendo uma promoção imperdível de máquina de lavar. Como tinha feito recentemente uma pesquisa, comparando preços e marcas desse produto, percebe que o valor do anúncio se encontra muito abaixo do praticado no mercado. Ao clicar é redirecionado para uma página muito semelhante a da americanas, que detalha melhor a promoção, explica que você deve aproveitar a oportunidade relâmpago, que é possível comprar com apenas um clique (não é necessário cadastro) e afirma que a única modalidade de pagamento é por meio de boleto bancário. Sendo assim, salienta que a promoção está acabando naquele mesmo dia e que restam apenas poucas unidades do produto em estoque. Após gerar o boleto bancário e efetuar o pagamento da compra você tenta acompanhar o envio do produto pelo número do pedido descrito no boleto. Porém, não consegue visualizar o pedido cadastrado para sua compra no site, entra em contato telefônico pelo canal de atendimento ao cliente e percebe que foi vítima de um golpe. De acordo com os conhecimentos adquiridos no curso identifique quais vulnerabilidades podem ter sido exploradas para enganar o usuário? Identifique quais estratégias de golpe foram utilizadas? Explique quais ações o usuário deveria ter adotado para identificar a fralde? O que deve ser feito caso o usuário efetue o pagamento do boleto fraudulento? \*

Sua resposta

Enviar

0 pontos

Nunca envie senhas pelo Formulários Google.

Este formulário foi criado em INSTITUTO FEDERAL DO PIAUÍ. D enunciar abuso

###### [Formulários](https://www.google.com/forms/about/?utm_source=product&amp;utm_medium=forms_logo&amp;utm_campaign=forms)

X



[Curso em Segurança da Informação](https://mooc-seginfo.appspot.com/moocseg/)

[williamdasilvamelo@gmail.com](mailto:williamdasilvamelo@gmail.com) | [Dashboard](https://mooc-seginfo.appspot.com/moocseg/dashboard) | Sair

[Notificações](https://mooc-seginfo.appspot.com/moocseg/announcements) [**Curso**](https://mooc-seginfo.appspot.com/moocseg/course)[Progresso](https://mooc-seginfo.appspot.com/moocseg/student/home)

**Search**

**Prova Final** [](https://mooc-seginfo.appspot.com/moocseg/dashboard?action=edit_assessment&amp;key=45)

**Data de entrega desta tarefa:** 2025-01-01, 03:00 UTC.



informações com fim de preservação ou valor que possui para um indivíduo ou organização. Quais são os três pilares básicos de segurança da informação, escolha abaixo a alternativa correta.

Integridade, usabilidade e simplicidade Confidencialidade, integridade e disponibilidade Confidencialidade, autenticação e disponibilidade Rastreabilidade, usabilidade e notoreidade Disponibilidade, rastreabilidade e simplicidade

2. Considere o texto a seguir: “Uma falha ou fraude no procedimento, design, implementação, *Um ponto* ou controles internos de um sistema que podem ser acidentalmente ou propositalmente explorados, resultando em uma violação de segurança ou violação da política de segurança do sistema”. No contexto de segurança da informação, essa é uma definição de:

Risco Vulnerabilidade Impacto Ameaça

Engenharia social

*Um ponto*

Fala sobre os conceitos e princípios em segurança da informação.

1. A Segurança da Informação (SI) é especializada na proteção de um conjunto de



Códigos maliciosos

1. Um Técnico de Informática está analisando como recursos de diversas pragas virtuais *Um ponto*

(malwares), para executar a instalação do antivírus adequado. Dentre as características específicas por ele analisadas, estão: I. Programa que, além de executar as funções para as quais foram executadas, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário. Um exemplo é um programa que recebe ou obtém sites na Internet e que parece ser inofensivo. Esse programa geralmente consiste em um único arquivo e é explicitamente executado para que seja instalado no computador. II. Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído na ação de outros códigos maliciosos, que podem afetar o computador ou atacantes que exploram vulnerabilidades existentes nos programas utilizados no computador. Após incluído, ele é usado para garantir o acesso futuro ao computador comprometido, permitir que ele seja acessado remotamente, caso haja necessidade de executar novamente os métodos de execução de invasão ou infecção e, na maioria dos casos, sem que seja notado. III Programa que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia. O atacante exige pagamento de resgate para restabelecer o acesso ao usuário. As descrições acima são, corretas e respectivamente, correspondentes a

Worm, backdoor e vírus

Spyware, cavalo de Troia (trojan) e ransomware Vírus, spyware e rootkit

Cavalo de Troia (trojan), backdoor e ransomware Bot, Rootkit e cavalo de Tróia (Trojan)

1. O é um programa capaz de se propagar automaticamente pelas redes, *Um ponto*

enviando cópias de si mesmo de computador para computador. É notadamente responsável por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costuma propagar e, como consequência, pode afetar o desempenho da rede e a utilização do computador.Assinale a alternativa que CORRETAMENTE preenche a lacuna do texto acima.

Worm Keylogger Vírus Trojan Spyware

1. Existem diversos tipos de códigos maliciosos, entre eles o spyware. Acerca desse assunto, *Um ponto*

é correto afirmar que spyware consiste em:

Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

Programa que além de projetar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, sem o conhecimento do usuário.

Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para esse fim.

Programa ou parte de um programa de computador, normalmente malicioso, que se propaga, inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos.

1. E-mail spoofing é uma técnica que pode ser utilizada para propagação de códigos maliciosos, envio de spam e golpes de phishing. Esta técnica consiste em:

*Um ponto*

alterar as configurações de um servidor de e-mail para que dispare uma infinidade de e-mails falsos até encher a caixa de correio de um ou muitos usuários

Alterar os campos do protocolo SMTP, de forma que os e-mails do usuário sejam direcionados para outra sem que ele saiba.

Efetuar buscas minuciosas no computador do usuário, com o objetivo de identificar informações sigilosas.

Alterar os campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

falsificar o protocolo SMTP para inspecionar os dados trafegados na caixa de e-mail do usuário, por meio do uso de programas específicos.

1. Das alternativas a seguir, assinale a única que contém eventos que caracterizam uma tentativa de ataque do tipo força bruta.

*Um ponto*

Brechas resultantes de bugs no sistema



A operação local e não autorizada de estações ou servidores

Sobrecarga de servidores, alcançada por meio de ataques simultâneos e descentralizados

A repetição automática de tentativas de acesso a um recurso protegido, com senhas criadas a partir de combinações aleaórias ou extraídas de listas pré-definidas.

A captura de dados sensíveis a partir de um programa espião instalado no computador do usuário.

1. Vários computadores de uma rede estão gerando spam, disseminando vírus, atacando *Um ponto*

computadores e servidores de forma não prevista pelos administradores. Foi identificado um malware que é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados nos computadores infectados, tornando-os zumbis. Tal comportamento é tipicamente ocasionado por uma ação de

Spyware Keylogger Phishing Botnet Adware

1. Spam e Spyware são basicamente: *Um ponto*

Dois softwares do typo player de vídeo

Dois tipos de vírus fatais que podem danificar um computador. Respectivamente, um programa espião e um e-mail não solicitado Respectivamente, um e-mail espião e um vírus de computador.

Respectivamente, um e-mail não solicitado e um programa espião.

1. A técnica de Sniffing *Um ponto*

Captura e inspeciona dados que trafegam em uma rede Tenta adivinhar por tentativa e erro a senha de um usuário.



Altera campos do cabeçalho de mensagens de e-mail para falsificar a origem da mensagem Utiliza um ou mais computadores para tornar indisponível um serviço provido.

Altera o conteúdo de páginas web de forma maliciosa e publica informações contra a instituição mantenedora da página web.

**Conferir respostas**

**Enviar respostas**

Avaliação do curso

\*Obrigatório



Endereço de e-mail \*

Seu e-mail



01 - De uma forma geral, considerando a escala abaixo informe seu grau de

satisfação com o curso online de segurança da informação \*

1

2

3

4

5

6

7

8

9

10



02 - Seu grau de satisfação considerando o conteúdo do curso \*

1 ponto

1

2

3

4

5

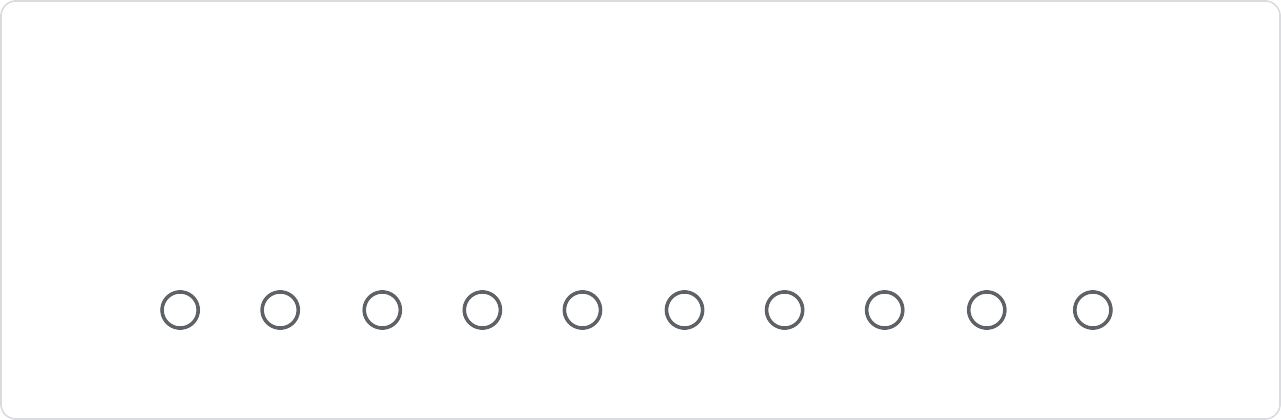
6

7

8

9

10



03 - Seu grau de satisfação considerando a as mídias e elementos utilizados no

curso \*

1

2

3

4

5

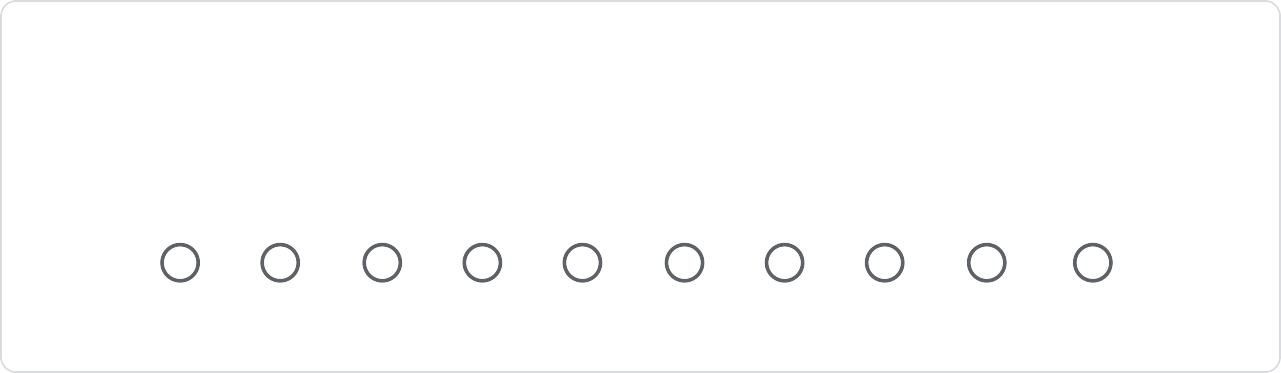
6

7

8

9

10



04 - Seu grau de satisfação considerando o material de leitura? \*

1

2

3

4

5

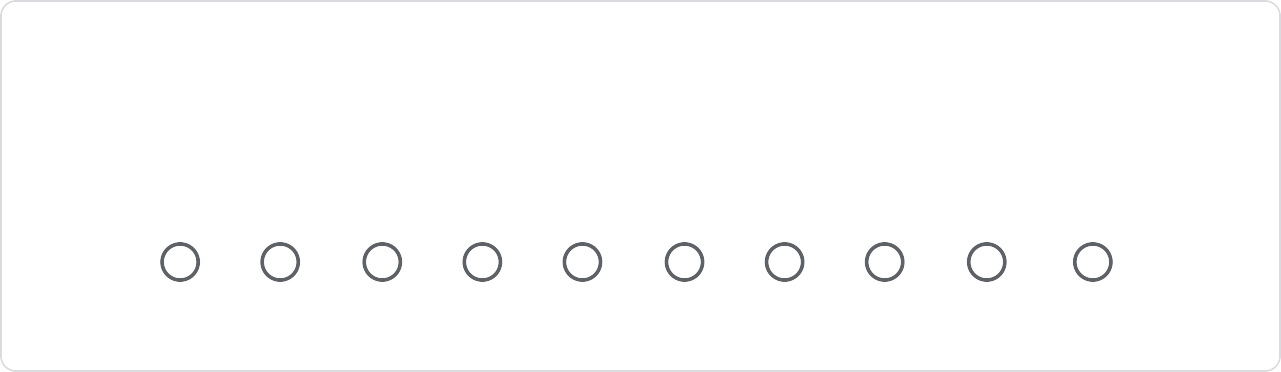
6

7

8

9

10



05 - Seu grau de satisfação considerando os desafios práticos? \*

1

2

3

4

5

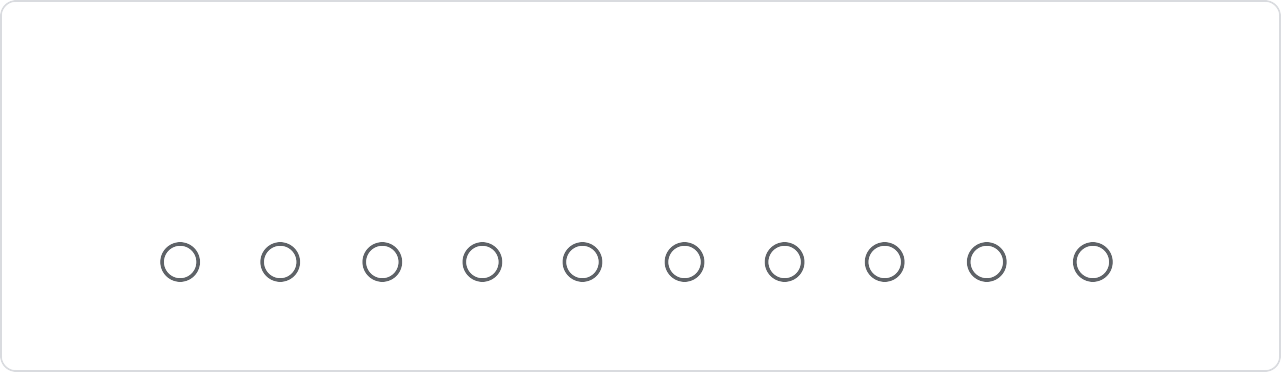
6

7

8

9

10



06 - Seu grau de satisfação considerando os estudos de caso? \*

1

2

3

4

5

6

7

8

9

10



07 - Seu grau de satisfação considerando o jogo de criptografia? \*

1

2

3

4

5

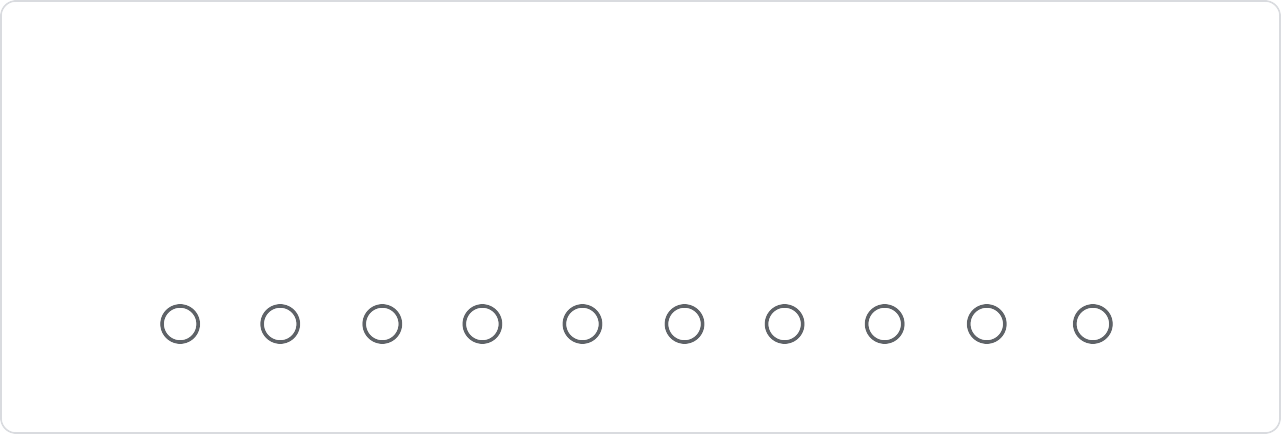
6

7

8

9

10



08 - Seu grau de satisfação considerando as discussões no grupo do Whatsapp?

\*

1

2

3

4

5

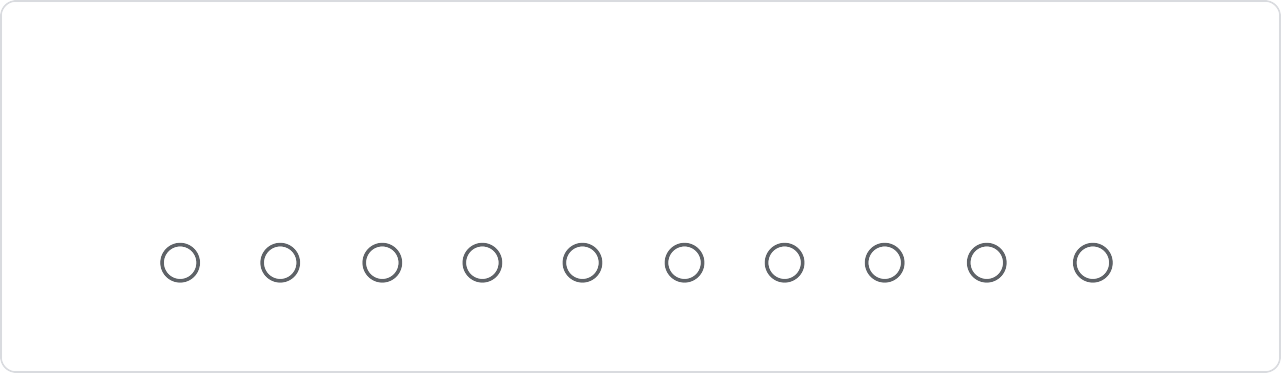
6

7

8

9

10



09 - Seu grau de satisfação considerando o material em vídeo? \*

1

2

3

4

5

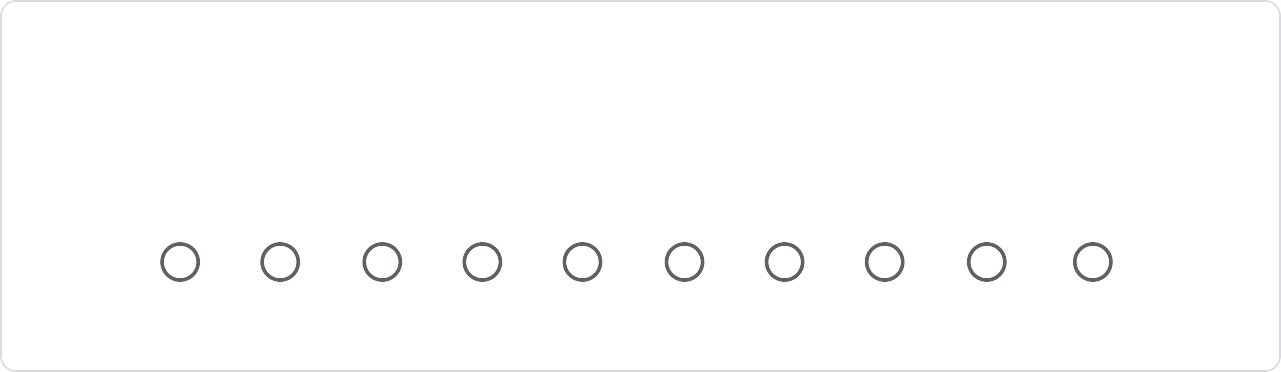
6

7

8

9

10



10 - Seu grau de satisfação considerando a interatividade do curso? \*

1

2

3

4

5

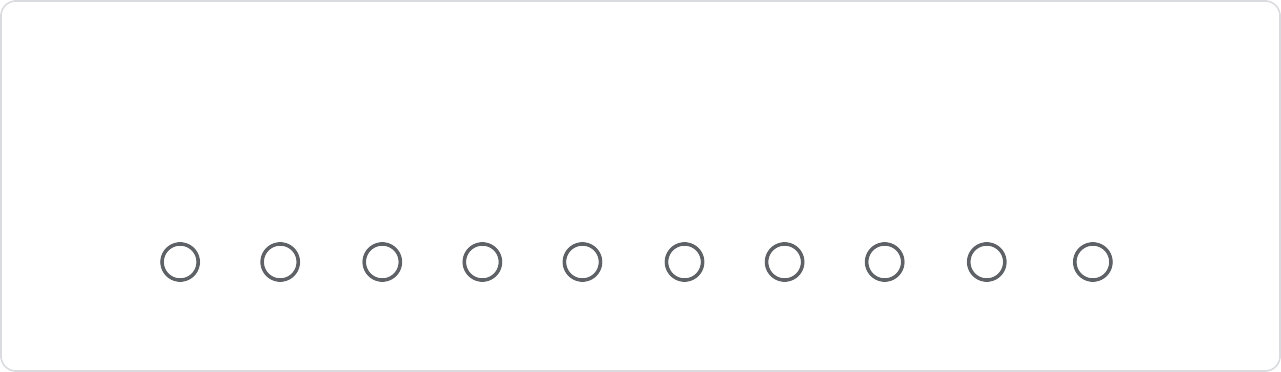
6

7

8

9

10



11 - Seu grau de satisfação considerando a duração do curso? \*

1

2

3

4

5

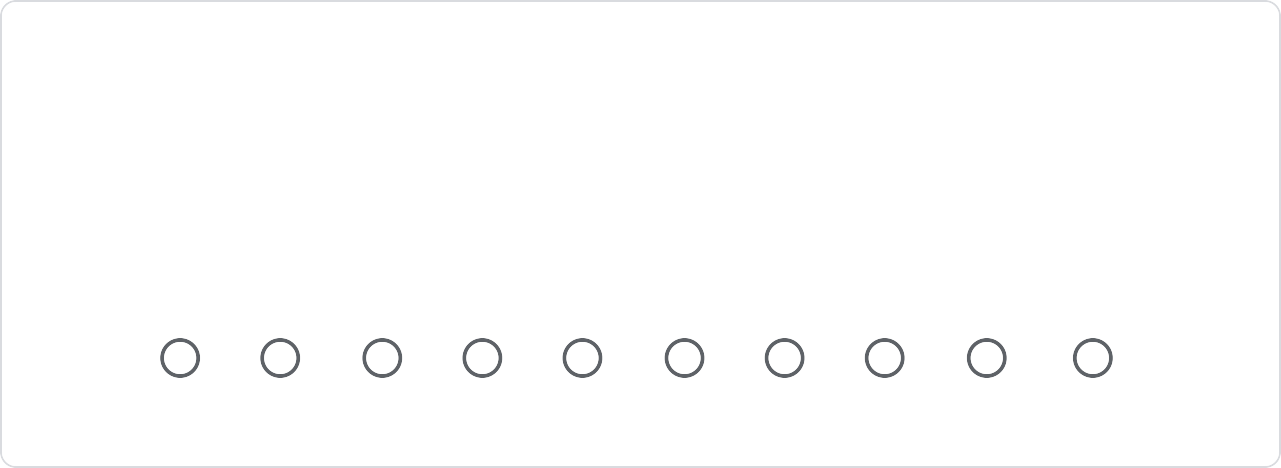
6

7

8

9

10



12 - A forma de apresentar as informações utilizando material de leitura, vídeos,

estudos de caso, jogos, trabalhos em grupo e desafios práticos permitiu aliar teoria e prática. \*

1

2

3

4

5

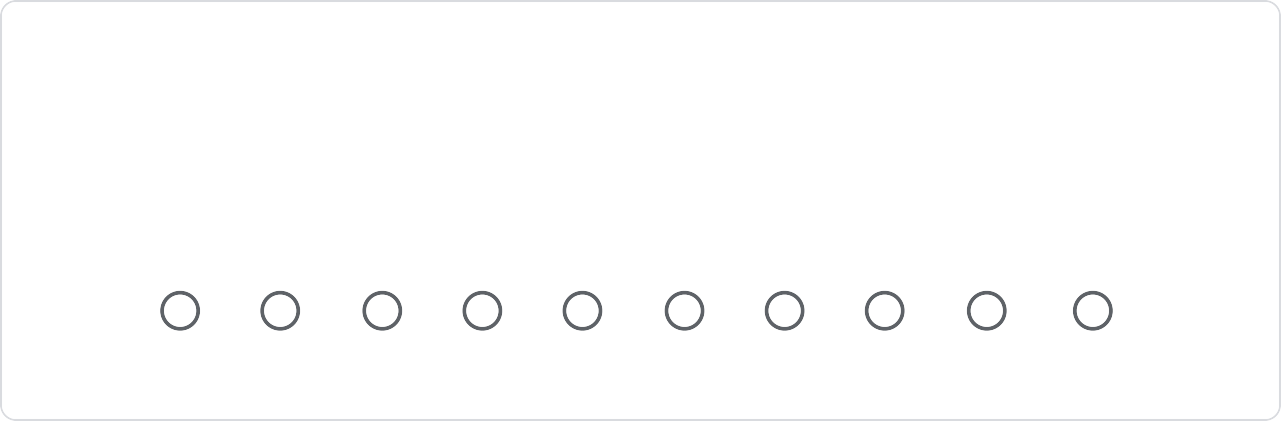
6

7

8

9

10



13 - O fórum de discussão foi uma ferramenta útil para tirar dúvidas, socializar ou

discutir sobre os temas abordados no curso \*

1

2

3

4

5

6

7

8

9

10

O que você achou do curso? \*

Sua resposta

Enviar

Nunca envie senhas pelo Formulários Google.

Este formulário foi criado em INSTITUTO FEDERAL DO PIAUÍ. D enunciar abuso

[Formulários](https://www.google.com/forms/about/?utm_source=product&amp;utm_medium=forms_logo&amp;utm_campaign=forms)