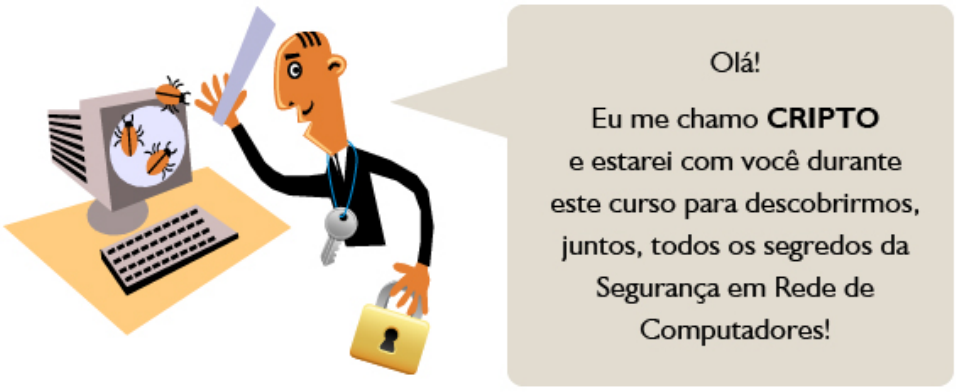
# Segurança em Redes

## Aula 01 - Introdução à Segurança

# Apresentação




Nesta disciplina, apresentaremos os conceitos necessários para você entender a terminologia, os ataques mais conhecidos, bem como seus mecanismos de defesa. Nas primeiras aulas, apresentaremos os conceitos básicos sobre atacantes, ataques e terminologia de segurança em rede e, ao longo do curso, apresentaremos os principais mecanismos de segurança. Ao final do curso, você terá conhecimento dos principais problemas de segurança em redes e como eles são prevenidos ou resolvidos. Esta disciplina não tem finalidade de esgotar toda a imensa gama de informações da área de segurança, mas, certamente, proporcionará uma formação geral que lhe permitirá conhecer os termos da área e a forma de operacionalizar os principais mecanismos de segurança.

Na primeira aula, iremos falar dos conceitos básicos de segurança, para que você tenha familiaridade com o tema.

## Objetivos

- Definir o objetivo das redes industriais.
- Descrever como acontece o processo de transmissão dos dados os seus formatos e modos de operação.
- Identificar como é feita a verificação de erros.
- Exemplificar a forma do tráfego de dados.

# Conceitos de Segurança

Os usuários de um ambiente computacional devem conhecer, mesmo que minimamente, a necessidade de proteger seus arquivos, programas e dados que fluem através da internet. É comum ficarmos apavorados ao pensar que nosso computador, nossos dados ou nossos programas foram vítimas de vírus, ou de algum outro problema relacionado à segurança, que venham a impedir o correto funcionamento do computador ou ocasionar a perda ou o roubo de informações.

A área de **Segurança Computacional** define um conjunto de normas, procedimentos e posturas que têm por objetivo prevenir ou monitorar a ação de usuários mal-intencionados (*atacantes* ou *intrusos*). Dessa forma, podemos evitar que eles alcancem seus objetivos através do *acesso não autorizado* ou *uso não autorizado* de computadores e suas redes (HOWARD, 1997), ou minimizar os danos ocorridos. O **acesso não autorizado** acontece quando alguém acessa o ambiente computacional (dados ou recursos computacionais, como impressoras, discos etc.) sem ter autorização. O **uso não autorizado** acontece quando alguém, que tem autorização para acesso a um sistema, realiza alguma ação que não é permitida. Por exemplo, um administrador de rede tem acesso a todos os dados dos usuários da rede, mas ele não pode olhar e-mails ou abrir arquivos pessoais desses usuários, nem fazer qualquer ação que seja uma invasão de privacidade.

O problema de segurança em ambientes computacionais é antigo, mas ficou ainda mais grave com a popularização das redes de computadores, principalmente a internet. Antes dessa popularização as ameaças de segurança exigiam alguma interação física entre o atacante e o computador atacado (como a inserção de um disquete no drive do computador). Com o uso das redes, passou-se a ter necessidade de proteger o ambiente dos ataques que podem vir através dela. O termo **Segurança em Redes** refere-se a “formas de proteção para prevenir, deter e corrigir violações de segurança que envolve a transmissão via rede” (STALLINGS, 2010).

**Vídeo 01** - O Que é Segurança?

# Atividade 01

1. Você sabe a diferença entre segurança computacional e segurança em redes?

# Ameaças

Uma **ameaça** é a possibilidade de uma **vulnerabilidade** ser explorada por um **atacante**. Já uma **vulnerabilidade** é uma fraqueza de um ou mais componentes de um sistema (computador ou rede) que podem ser explorados por um **atacante** afetando a confidencialidade, integridade ou disponibilidade dos dados. Esses três termos são conhecidos como **serviços de segurança**, e podem ser definidos basicamente como:

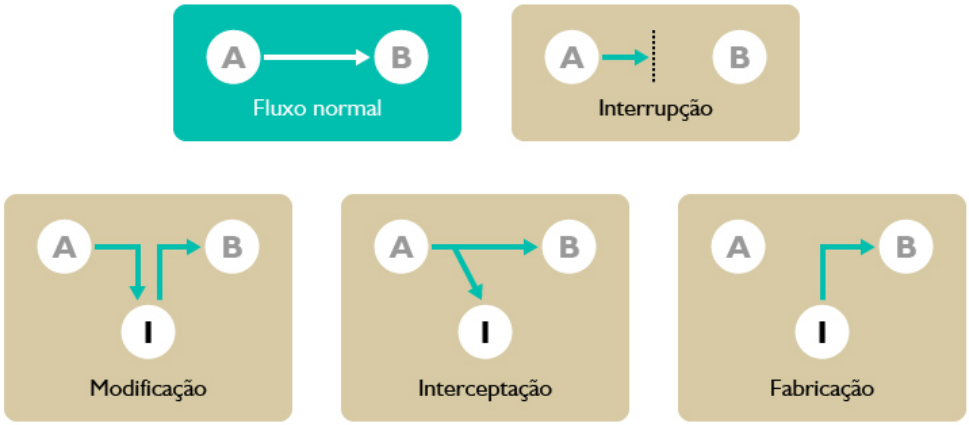
1. **Confidencialidade:** sua finalidade é garantir que apenas usuários autorizados tenham acesso à informação. Ou seja, é um serviço que garante o sigilo das informações. Um exemplo típico de necessidade de confidencialidade são as contas bancárias. Um serviço de segurança deve garantir que apenas o proprietário da conta tenha acesso ao extrato bancário. Outro exemplo é o caso de um arquivo com a prova de uma disciplina. O professor precisa ter a garantia de que o arquivo é confidencial e nenhum aluno vai ter acesso a esse arquivo antes da hora da prova.

2. **Integridade:** sua finalidade é garantir que apenas usuários autorizados possam modificar informações (escrever, apagar etc.). Por exemplo, no caso do arquivo com a prova, apenas o professor deve poder alterar o conteúdo ou mesmo apagar o arquivo.

3. **Disponibilidade:** a finalidade é garantir que os recursos computacionais e as informações estejam acessíveis e prontos para uso. Ou seja, um serviço que garanta disponibilidade deve proteger o sistema para que ele não seja degradado ou se torne indisponível, e o usuário tenha acesso ao sistema e aos dados sempre que precisar. Atacar a disponibilidade significa realizar ações que acarretem a negação do acesso a um serviço ou informação. Por exemplo, enviar um número enorme de mensagens para um servidor faz com que tal servidor fique sobrecarregado e não consiga atender à solicitação, tornando o serviço fornecido indisponível.

Por fim, o **ataque** é a técnica utilizada para explorar uma vulnerabilidade. Segundo Stallings (1999), ataques podem ser classificados, de forma teórica, em quatro grandes categorias. A Figura 1 mostra o fluxo normal das informações, realçado na cor verde, e as quatro grandes categorias de ataques.

**Figura 01** - Tipos de Ataques




**Fonte**: Stallings (1999, p. 7).

- **Interrupção**: o fluxo de mensagem é interrompido. Por exemplo, um usuário A envia uma mensagem para o usuário B e a mensagem não chega ao destino devido a algum tipo de ataque, por exemplo, o corte de uma linha de comunicação entre A e B. Essa categoria de ataque afeta a disponibilidade.

- **Interceptação**: um usuário A envia uma mensagem para outro usuário B. Durante o envio, um usuário intruso I intercepta e tem acesso à mensagem, afetando sua confidencialidade. Nesse caso, nem o usuário A nem o usuário B percebem a interceptação. Um exemplo seria a captura de dados na rede ou a cópia ilegal de um arquivo.

- **Modificação**: um usuário não autorizado, além de interceptar uma mensagem, a altera e reenvia para o destinatário, afetando sua integridade. O usuário A envia uma mensagem ao usuário B e a mensagem é capturada por um usuário intruso I que a modifica e a envia ao usuário B.

- **Fabricação**: um usuário não autorizado cria uma mensagem e a insere no sistema se passando por outro usuário. Por exemplo, o usuário intruso I envia uma mensagem para o usuário B como se fosse o usuário A. Nesse exemplo, o usuário intruso I está se passando pelo usuário A, realizando uma personificação *(ou spoofing).*

Ainda nesta aula veremos exemplos reais de tipos de ataques bastante comuns nos dias atuais.

# Atividade 02

1. Diferencie modificação de fabricação.

# Tipos de Atacantes

O termo atualmente mais conhecido e utilizado para denominar quem realiza ataques a sistemas computacionais é ***hacker***, mas essa definição não é totalmente adequada. O termo *hacker* tem origem na expressão "*to hack*",e a tradução mais próxima seria "fuçar". O termo *hacker* nasceu na década de 1960 e descrevia genericamente comunidades de estudantes e profissionais entusiastas das áreas de *software* e *hardware*. Das ideias e trabalho dessas comunidades surgiu o movimento do *software* livre, a *World Wide Web* etc. Uma definição intermediária é dada por Emilio Tissato Nakamura, em seu livro intitulado *Segurança de Redes em ambientes cooperativos*. Segundo ele, *hackers* seriam aqueles que usam de seus conhecimentos para atacar sistemas, não com o intuito de causar danos às suas vítimas, mas sim como uma forma de testar os seus limites e habilidades. Ao contrário dos *hackers,* os *crackers* atacam sistemas com o objetivo de roubar informações e causar danos às suas vítimas, seja para ter retorno financeiro ou simplesmente para divertimento malicioso.

Pesquisando em livros ou na internet, iremos encontrar diversas classificações de tipos de atacantes. Essas classificações normalmente levam em conta o nível de conhecimento e intenções do atacante, quando realiza ataques a sistemas. A seguir, iremos listar alguns dos tipos de atacantes mais comuns:

- ***Script kiddies*** (*garotos de script,* em tradução literal): é um termo depreciativo usado para se referir a *crackers* inexperientes. São também conhecidos como *newbies* (ou iniciantes). Por serem inexperientes, utilizam apenas ferramentas de ataque desenvolvidas por outras pessoas e obtidas na internet, sem saberem exatamente o que estão fazendo.

- ***Cyberpunks***: são aqueles que realizam ataques por puro divertimento e desafio. Geralmente também são os responsáveis por encontrar vulnerabilidades em sistemas e divulgá-las na internet, trazendo um benefício às organizações (que podem então consertá-las). Normalmente esse termo também é aplicado para *crackers* paranoicos, que acreditam em teorias da conspiração e na possibilidade dos governos "vigiarem" todas as comunicações entre cidadãos. Suas ações também tem um cunho de protesto.

- ***Insiders***: são os responsáveis por ataques de dentro da própria organização, sendo os principais responsáveis pelos maiores prejuízos com fraudes financeiras e com abusos nas redes internas. Os *insiders* geralmente são funcionários descontentes com seu trabalho e normalmente os principais autores da espionagem industrial, que é considerada uma nova modalidade de crime.

- ***White-hats*** (chapéus brancos, em tradução literal): usam seus conhecimentos para descobrir problemas de segurança e aplicar as correções necessárias, agindo sempre dentro da lei. Normalmente eles são contratados pelas empresas para fazer testes e simulações para medir o nível de segurança das redes. São comparados a policiais que buscam falhas em sistemas a fim de corrigi-las. É comum encontrá-los ministrando palestras sobre segurança de sistemas ou trabalhando em empresas para garantir a segurança.

- ***Black-hats***: (chapéus pretos, em tradução literal): também conhecidos como *full fledged* ou *crackers*, eles usam seus conhecimentos em benefício próprio e, geralmente, realizam ataques com objetivos ilícitos, como o roubo de informações secretas de organizações. Ações como quebrar a segurança de um

programa, ou seja, fazer com que o programa não precise ser mais pago, são comuns dos *black-hats.* Ao contrário dos *white-hats*, os *black-hats* são *hackers* criminosos.

**Vídeo 02** - Tipos de Atacantes

## Atividade 03

1. Em suas palavras, diga a diferença entre um hacker e um cracker.

## Principais Tipos de Ataques

Um atacante pode causar diversos tipos de problemas às suas vítimas – desde simples transtornos até grandes prejuízos financeiros. Existe uma terminologia específica no mundo da segurança que é usada para classificar os ataques, e muitos desses termos são de amplo conhecimento da sociedade. Primeiramente iremos dividir os ataques em dois grandes grupos:

- **Ataques locais**: são aqueles originados diretamente na máquina que está sendo atacada.
- **Ataques remotos**: são aqueles que podem ser originados de qualquer máquina conectada à internet.

A seguir, iremos listar alguns exemplos desses dois grupos de ataques com suas definições.

**Vírus**: é um tipo de ataque local, realizado por um *software* malicioso que pode destruir dados, alterar o funcionamento de *softwares* e (raramente) danificar *hardware*. Vírus podem se replicar

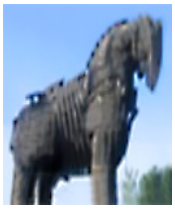
e passar de um computador para outro. Um vírus é um termo muito conhecido dentro da computação, mas acaba sendo confundido com um verme ou cavalo de troia.

A contaminação de um computador por um vírus requer alguma interação do usuário, por exemplo: (i) o usuário executa um arquivo infectado recebido em um anexo de um e-mail; (ii) o usuário utiliza arquivos infectados em *pen drives* ou CDs; (iii) o computador do usuário está com o sistema operacional desatualizado, sem correções de segurança que o fabricante normalmente disponibiliza, que corrigem vulnerabilidades conhecidas. Atualmente, existem milhares de vírus conhecidos, sendo a tarefa de detectá-los e removê-los do sistema normalmente realizada por um tipo de ferramenta de defesa chamada de antivírus.

## Curiosidades

1. O primeiro vírus de que se tem notícia era chamado de “Crepper Virus” e infectou computadores conectados à rede ARPANET na década de 1970. Ele simplesmente imprimia a mensagem *“I’m the creeper, catch me if you can!”* nos computadores infectados.
2. Em torno de 2006 e 2007 houve muitas ocorrências de vírus capazes de enviar *scraps* (recados) automaticamente para todos os contatos da vítima na rede social Orkut. Apesar de a vítima precisar clicar em um link malicioso inserido no recado para se contaminar, a probabilidade disso acontecer era muito alta, dada a relação de confiança entre amigos. Esses vírus normalmente roubavam senhas, como as de e-mail, ou até mesmo de contas bancárias dos usuários do computador infectado. Isso era feito através da captura de teclas digitadas e cliques do mouse. (WIKIPÉDIA, 2010a, extraído da internet e adaptado).

**Cavalo de troia**: da mesma forma que o mitológico cavalo de Troia parecia ser um presente, mas na verdade escondia soldados



gregos em seu interior que tomaram a cidade, os cavalos de troia atuais são outro tipo de ataque local, realizado por programas de computador que parecem legítimos, mas na verdade escondem funcionalidades que comprometem a segurança. Diferentemente de vírus, eles não criam réplicas.

Os danos causados vão desde o envio de senhas e arquivos (do computador atacado para o atacante) até a abertura de portas para futuras invasões e instalação de programas para que o atacante tenha controle total sobre o computador atacado. Recentemente, surgiu uma nova variante remota desse tipo de ataque conhecida como *phishing*, caracterizada pelo envio de mensagens de e-mail solicitando dados pessoais, tais como senhas ou números de cartões de crédito dos usuários ou a instalação de alguma "ferramenta de segurança".

**Exemplo real de um ataque:** usuários com conta de e-mail no provedor UFRNet têm recebido, frequentemente, o e-mail a seguir, solicitando os dados da conta, inclusive senha.

```
from     ufrn <ufrn@ufrn.br>
reply-to     wwebmaster@w.cn
To
Date    Tue, Aug 3, 2010 at 9:05 PM
Subject  UFRN Email Atualizando
mailed-by    ufrn.br

da conta de e-mail da UFRN que se recusa a atualização de contas
de e-mail dentro de 48 horas após o recebimento desta advertência
perderá conta de e-mail permanente. Por favor, envie-nos as suas
informações UFRN abaixo para atualização e requalificação. Logo
que recebermos o seu e-mail informações UFRN abaixo, vamos
chamá-lo pelo telefone para confirmar.
========================
Nome completo:
Número de telefone:
E-mail:
Senha E-mail:
========================
```

## Curiosidade

A ideia do *phishing* é “pescar” dados de usuários desatentos que caem na cilada. É inspirado no inglês “*to fish*” (pescar). No caso do *phishing*, os *crackers* têm a mesma função dos pescadores, que jogam uma isca para conseguir peixes.

**Vídeo 03** - Tipos de Ataques

# Atividade 04

1. Você consegue imaginar maneiras de nunca ser vítima de um phishing? Quais?

# Principais Tipos de Ataques

***Password crackers*:** são programas desenvolvidos para tentar descobrir a senha de um ou mais usuários, principalmente aqueles que possuam permissão de administrador. Funcionam pela realização de inúmeras tentativas, em um método conhecido como “força bruta”. Apesar de ser considerado um ataque local, atualmente também pode ser aplicado remotamente.

**Engenharia social:** conjunto de métodos não técnicos para obter acesso a um sistema ou informação não autorizada. Por exemplo, um atacante com boa lábia (ou cara de pau) pode tentar se passar por recém-contratado da empresa, para ter acesso à sala do diretor e, dessa forma, ao seu computador. Outro atacante pode

utilizar dados obtidos na internet, por exemplo, em perfis de redes sociais, e ligar para um provedor tentando se passar por um usuário, solicitando uma alteração de senha de e-mail.

***Worm* ou verme:** é similar a um vírus, porém tem capacidade de se replicar de forma automática, propagando-se através da internet e enviando cópias de si mesmo para outros computadores, sem a necessidade de interação com o usuário. O grande perigo dos vermes está exatamente na capacidade de se replicar em grande volume. Por exemplo, um *worm* pode enviar cópias de si mesmo a todos os computadores de uma rede local, alastrando-se rapidamente.

## Curiosidades

1. Um dos *worms* mais famosos da história foi o "*SQL Slammer*". Ele causou uma negação de serviço em milhares de servidores, chegando a degradar o tráfego da internet como um todo. Lançado em 25 de janeiro de 2003, ele infectou 75.000 servidores em apenas 10 minutos. Ele explorava uma vulnerabilidade existente em servidores Windows que possuíssem o servidor de bando de dados SQL Server instalado.
2. Além do *Slammer*, vejamos uma lista de outros vírus e *worms* "famosos":
    1. **Michelangelo – 1991:** espalhava-se por disquetes e ficava em um estado de "dormência" até o dia 06/03. Nesse dia "acordava" e destruía uma série de arquivos dos usuários.
    2. **ILOVEYOU – 2000:** considerado um dos vírus mais bem-sucedidos até os dias atuais, causou prejuízos de bilhões de dólares. Espalhava-se por e-mail, se reenviando para todos os contatos de um usuário infectado. Podia corromper arquivos de fotos, documentos de texto, planilhas etc.

3. **Sasser – 2004:** explorava uma vulnerabilidade não corrigida do Windows, espalhando-se pela rede (porta 445). Causou um grande caos, dado que os computadores infectados reiniciavam, ou travavam, poucos minutos depois de serem ligados (ou infectados).

4. **Conficker – 2008:** infectou, via rede, cerca de 15 milhões de computadores em todo o mundo. Computadores infectados podiam ser controlados remotamente por um "operador" para realizarem uma série de ações.

***Spywares*:** também pertence à classe dos vírus e *worms*, normalmente têm o objetivo de coletar informações pessoais do usuário e enviá-las ao atacante.

***Port scanners* e *scanners* de vulnerabilidades:** ataque remoto em que um programa tenta conectar em cada porta TCP/UDP possível, obtendo a lista de portas abertas de uma máquina. Opcionalmente podem tentar obter informações sobre as aplicações "escutando" em cada porta aberta, bem como do sistema operacional, e gerar uma lista de vulnerabilidades presentes na máquina atacada.

**Captura de tráfego (*sniffing*):** Captura remota de todos os pacotes que estão transitando destinados a uma máquina ou rede. Com sua captura e posterior análise pode-se visualizar todas as informações trocadas por serviços que não utilizam criptografia.

**Denial of Service (DoS):** ataque remoto cujo objetivo é interromper ou impedir totalmente o uso de um serviço por usuários legítimos. Funciona pelo envio de um número imenso de requisições a um ou mais servidores, de forma que ele não consiga respondê-las. Provoca um consumo anormal de recursos, como processamento, memória ou tráfego de rede. Pode ser realizado de forma distribuída, por vários atacantes ao mesmo tempo, sendo então chamado de *Distributed Denial of Service (DDos)*.

## Curiosidade

Esse tipo de ataque está sendo amplamente utilizado na atualidade por grupos *hackers*, como LulzSec e Anonymous. Sua estratégia básica é realizar ataques de DDoS contra sites de grandes empresas ou órgãos governamentais, tornando-os inacessíveis por algumas horas ou dias. O sucesso nos ataques é utilizado por esses grupos para permanecerem na mídia e divulgarem suas “ideias”.

**Ataques direcionados a aplicações web:** com o advento das páginas web dinâmicas e de linguagens específicas para o seu desenvolvimento, como ASP e PHP, surgiram oportunidades para novos tipos de ataques. Estes não são direcionados a um servidor ou serviço, mas diretamente às páginas que ele hospeda. Dentre esses ataques, podemos destacar os de ***Cross Site Scripting*** e ***SQL injection***, que têm como objetivo, por exemplo, a inserção de links ou códigos maliciosos em uma página. Através deles também é possível o acesso ou modificação não autorizada das informações existentes em um banco de dados que alimenta a página.

# Atividade 05

1. Você entendeu a diferença ente ataques locais e remotos? Dê exemplos dos dois tipos.

# Dicas de Segurança

Você precisa estar atento! Todos os dias centenas de vírus são criados e novos golpes são descobertos. Por isso, você precisa proteger seu computador dessas ameaças. A seguir, daremos algumas dicas para manter seus dados e computador

em segurança.

- **Sair de um site usando *Logout*, "Sair" ou equivalente**

Ao acessar seu e-mail, sites de bancos ou de comércio eletrônico, ou qualquer serviço que exija que você forneça um nome de usuário e uma senha, clique no botão ou link de nome *Logout*, Sair, Desconectar ou equivalente para sair do site. Nunca simplesmente saia do site, fechando a janela do navegador de internet ou entrando em outro endereço.

- **Crie sempre senhas difíceis**

Nunca use senhas fáceis de serem descobertas, como data de aniversário, nome de parentes ou sequências (ex.: 12345). Quanto mais fácil for a sua senha, mais fácil ocorrerá algum tipo de ataque. Sempre utilize senhas que misturam números e letras e caracteres especiais, como: @ % & #.

- **Cuidado com e-mails**

Sempre desconfie de e-mails de organizações ligadas ao governo, como TSE, TRT etc. Essas organizações não costumam mandar e-mails, principalmente pedindo dados pessoais. Sempre desconfie de possíveis prêmios que você possa ter recebido por e-mail.

- **Evite sites de conteúdo duvidoso**

Muitos sites contêm *scripts* capazes de explorar falhas do navegador de internet. Por isso, evite navegar em sites pornográficos, *hackers* ou que tenham qualquer conteúdo duvidoso.

- **Tenha e atualize sempre seu antivírus**

Sempre tenha um antivírus instalado em seu computador e sempre o mantenha atualizado. Muita gente pensa que basta instalar um antivírus em seu computador que estará protegido, mas não é assim. É sempre necessário atualizá-lo utilizando a internet, do contrário o antivírus não saberá da existência de vírus novos.

- **Não execute nem baixe arquivos não solicitados**

Vários ataques vêm embutidos em arquivos enviados via e-mail. Nunca baixe nem execute arquivos não solicitados. Arquivos que têm a extensão .exe, .scr, .pif, .cmd, .com, .cpl, .bat, .vir, entre outros, podem carregar consigo diversos tipos de ataques.

---

Você achou a aula legal?

Não é surpreendente que o mundo virtual é cheio de perigos? O mundo da Segurança em Redes é muito extenso e, nesta primeira aula, você aprendeu alguns conceitos importantes. Ainda há um "mar de informações" sobre o tema. Para maiores detalhes, veja as sugestões de leituras complementares!

## Leitura Complementar

- <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-pt_br-4/pt-general-intro.html>: Uma introdução genérica à segurança.
- <http://www.infowester.com/virus.php>: Sobre vírus.
- <http://pt.wikipedia.org/wiki/Phishing>: Sobre *phishing*.

# Atividade 06

---

Agora, vamos pesquisar.

1. Você sabe o que são botnets? Pesquise e elabore um texto explicando o que são.

# Resumo

Nesta aula, definimos Segurança em Redes e sua importância no mundo atual. Também vimos definições de ameaças, ataques e atacantes, além dos vários tipos de ataques e atacantes existentes. Por fim, apresentamos algumas dicas de segurança para ajudá-lo a proteger seu computador de possíveis ameaças.

# Autoavaliação

1. Explique o que é confidencialidade. Dê exemplos de situações onde ela é utilizada no seu dia a dia.
2. Qual era o significado do termo hacker quando de sua criação? Qual o significado atual?
3. Qual a principal diferença entre um vírus e um worm?
4. Explique, com suas palavras, o que são ataques de engenharia social.
5. O que é negação de serviço (DoS)? Qual a diferença para a DDoS?
6. Imagine os diversos tipos de prejuízos que os ataques estudados podem provocar. Liste aqueles que você conseguiu imaginar.

# Referências

AKAMURA, E.; GEUS, P. L. **Segurança em redes em ambientes cooperativos**. São Paulo: Editora Futura, 2003.

HOWARD, J. D. **An analysis of security incidents on the internet**: 1989-1995. 1997. Tese (Doutorado) – Carnegie Mellon University, Pittsburgh, Pennsylvania, 1997.

O QUE são vírus, worms e cavalos de Troia? Disponível em: <http://www.microsoft.com/brasil/athome/security/viruses/virus101.mspx>. Acesso em: 17 ago. 2010.

STALLINGS, W. **Cryptography and network security**: principles and practice. 5th. ed. New York: Prentice Hall, 1998. 744 p.

WIKIPÉDIA. **Phishing**. Disponível em: <http://pt.wikipedia.org/wiki/Phishing>. Acesso em: 31 ago. 2010a.