

# INFORMÁTICA

Proteção do Computador / Segurança da  
informação / Ameaças / Vulnerabilidades

**DISCIPLINA:  
INFORMÁTICA APLICADA**



**Docente: Rosana Barbosa**  
**[rosana@fatecba.edu.br](mailto:rosana@fatecba.edu.br)**



# As ameaças





# Inimigo número um: O usuário

Usuário é leigo, distraído e suscetível a ataques de engenharia social

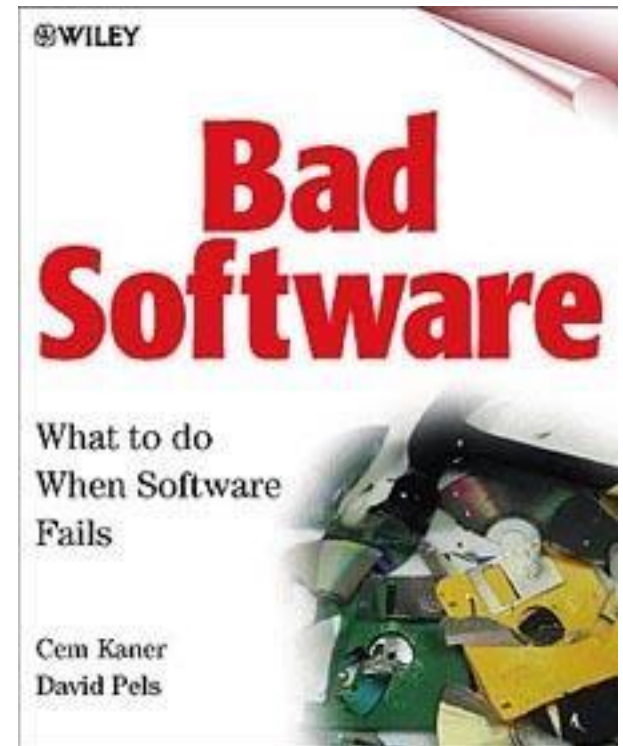
“Contra a estupidez, os próprios deuses lutam em vão”  
(Goethe)

# Inimigo número dois: software de má qualidade



- deixa o sistema (e o usuário) vulnerável
- software perfeito não existe
- software seguro é um mito
- importante manter-se atualizado

Bad, bad software  
no cookie for you



# Inimigo número três: vírus



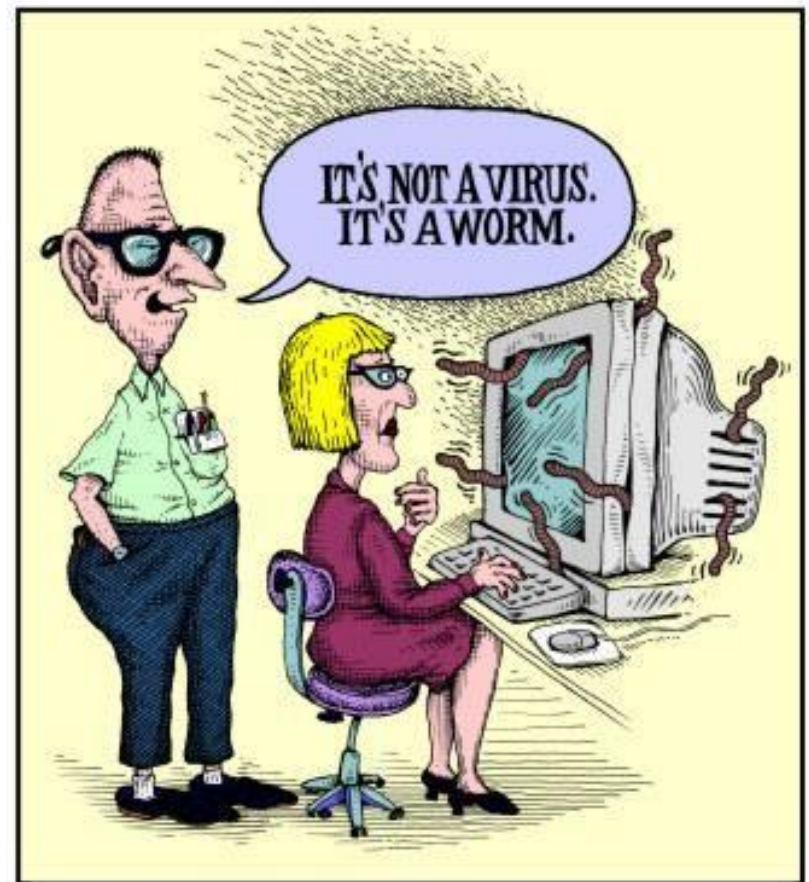
- vírus de boot
  - vírus de executável
  - vírus de macro  
(thanks, Microsoft!)
- 
- qualquer arquivo que contenha comandos pode ser infectado
  - usuário é um grande vetor de propagação de vírus (click me now!)



# • Inimigo número quatro: vermes



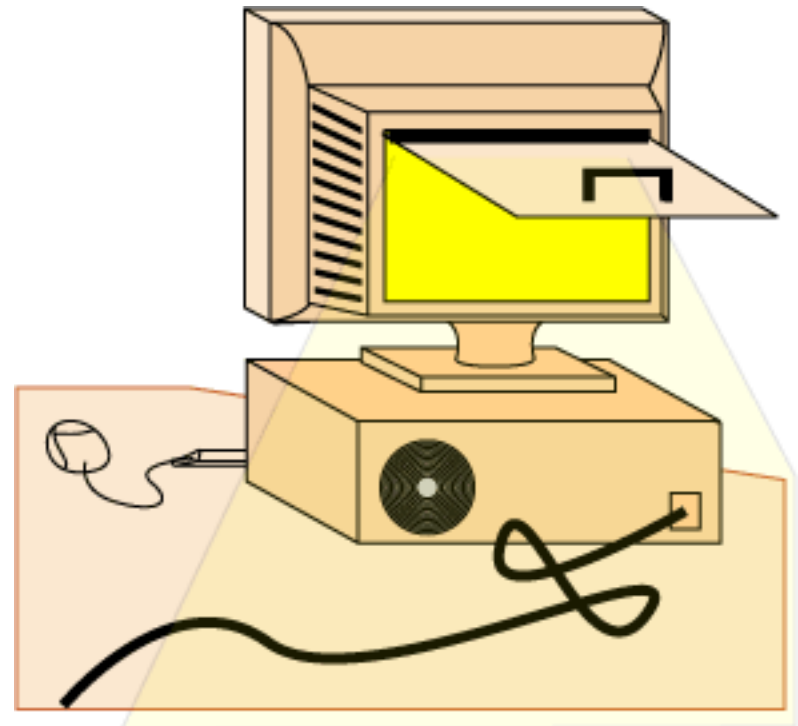
- propagam-se pela rede
- utilizam vulnerabilidades do sistema operacional ou dos serviços de rede (buffer overflow)
- usam o computador infectado como base para novas propagações



# • Inimigo número cinco backdoors



- instaladas por um programa daninho (ou um usuário distraído)
- deixam uma porta aberta para futuras invasões
- instalam “serviços” no computador





## • Inimigo número seis: hackers

- fama muito maior que a capacidade
- maioria são “script-kiddies” ou “one-click hackers”
- mas podem ser perigosos, principalmente se lhe escolherem como alvo



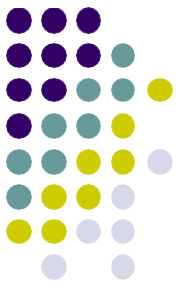
# • Inimigo número sete: spam e ataques à privacidade



- mais um incômodo que uma ameaça
- mas pode espalhar boatos
- difícil de controlar



**• Acompanhamos durante a pandemia o aumento de crimes virtuais. Calcula-se que, nos últimos meses, houve 23 ataques por minuto no Brasil. Com as pessoas em casa e o trabalho sendo executado remotamente, a troca de dados e informações foram feitas sem as devidas segurança.**



# FACEBOOK – VAZAMENTO DE DADOS



O Facebook teve dados vazados de cerca de 87 milhões de usuários no mundo inteiro, incluindo de 443 mil brasileiros. O caso só chegou a conhecimento público em 2018, mas as informações foram compartilhadas ilegalmente pela empresa Cambridge Analytica, responsável pelo tratamento de dados, em 2016 para manipulação eleitoral nos Estados Unidos.

# UBER – SEQUESTRO DE DADOS



●

A Uber sofreu um grande ciberataque em 2016. Houve exposição de informações pessoais de 57 milhões de usuários. Os dados foram sequestrados e a empresa precisou negociar com os responsáveis pelo ataque. Foi necessário pagar para que os dados fossem deletados, mas sem nenhuma segurança que os criminosos cumpririam com a palavra..

# Guerra cibernética



- O vírus Stuxnet é tão específico que especialistas crêem que ele foi criado pelos EUA ou Israel. Ele foi escrito para atacar apenas os sistemas das centrífugas de enriquecimento de urânio iranianas.



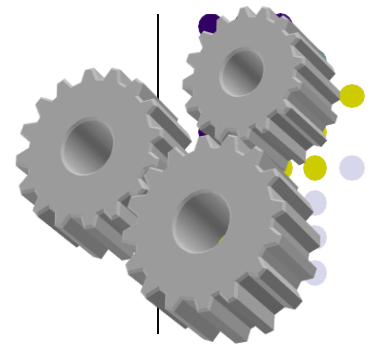


# Antivírus

- Detectar e então anular ou remover os vírus
- Alguns procuram remover e detectar cavalos de tróia e barrar programas hostis
- Verificar email (entrada e saída)
- Configure-o corretamente
- Algumas versões de antivírus são gratuitas e podem ser obtidas pela Internet. Mas antes, verifique sua procedência e certifique-se que o fabricante é confiável

Não impede a exploração de alguma vulnerabilidade e não é capaz de impedir o acesso a um *backdoor*

# Ferramentas Antivírus



- *Free AVG* – usuários domésticos
- *Free Avast Home Edition* – somente usuários domésticos
- *Nod32*
- *Norton Anti-vírus*
- Clam AntiVirus – toolkit anti-virus para Unix, para integração com servidores de e-mail (analisa os arquivos anexados)
  - <http://www.clamav.net/>

# Outras classificações de aplicativos



- Capturadores de teclas/tela (*Keyloggers, Screenloggers*)
  - Ficam residentes em memória capturando todas as teclas/telas que o usuário do sistema pressiona/visualiza
  - Envia essas informações para um usuário malicioso
- Aplicativos de propaganda (*Adwares*)
  - Ficam residentes em memória, lançando janelas *Pop-Up* com propagandas
  - As informações sobre as propagandas são atualizadas via rede
- Aplicativos espiões (*Spywares*)
  - Residentes em memória, monitoram o comportamento do usuário
    - Sites que ele navega, preferências, etc.
  - Envia essas informações para preparar uma mala-direta ou para ativar *Adwares*



# Dados estatísticos

Home > Segurança

**Em 2020, pelo menos 360 mil vírus para computador foram criados por dia**

Por Ramon De Souza | 25 de Dezembro de 2020 às 19h00

O que já era incrível ficou ainda mais

baixe agora!

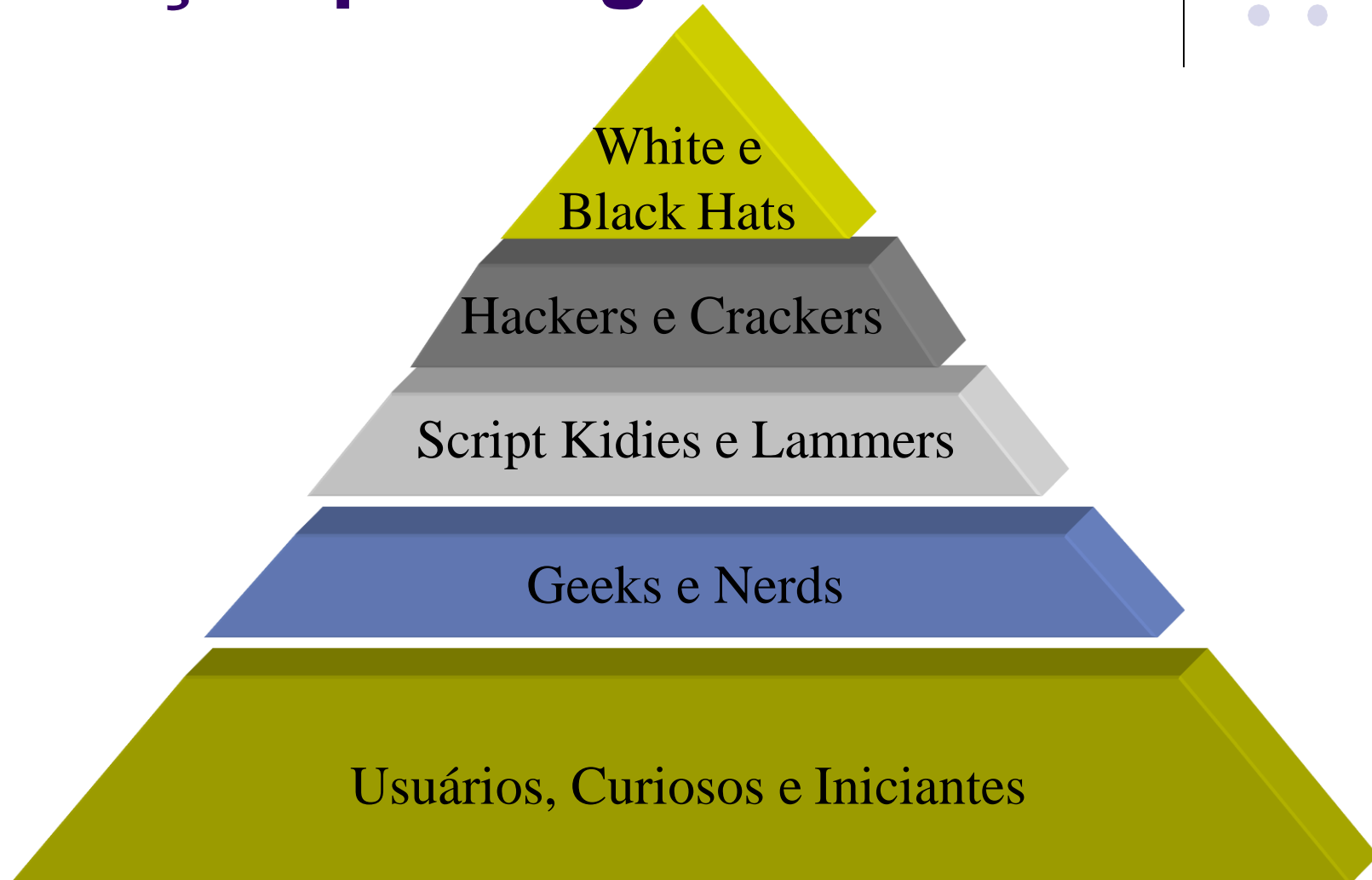
# HACKERS E CRACKERS



Originalmente, e para certos programadores, hackers (singular: hacker) são indivíduos que elaboram e modificam software e hardware de computadores.

Os hackers utilizam todo o seu conhecimento para melhorar softwares de forma legal. Eles geralmente são de classe média ou alta, com idade de 12 a 28 anos.

# População por segmento



# HACKERS E CRACKERS



O termo Cracker, do inglês "quebrador", originalmente significa alguém que "quebra" sistemas. Hoje em dia, pode tanto significar alguém que quebra sistemas de segurança na intenção de obter proveito pessoal (como por exemplo modificar um programa para que ele não precise mais ser pago).

# ● David L. Smith



Smith é o autor do notório "worm Melissa", responsável por sobrecarregar e tirar do ar vários servidores de e-mail em 1999. Smith foi detido e condenado em 2002 a 10 anos de prisão por ter causado mais de US\$80 milhões de prejuízo. A pena chegou a ser reduzida para 20 meses (mais multa de US\$ 5 mil) quando Smith aceitou trabalhar com o FBI, logo após sua captura. Inicialmente ele trabalhou 18 horas por semana, mas logo a demanda aumentou, fazendo-o trabalhar 40 horas semanais. Ele foi incumbido de obter conexões entre os autores de vírus novos, mantendo a atenção às vulnerabilidades dos softwares e contribuindo para a captura dos invasores.

# ● Kevin Poulsen



Seu principal feito aconteceu em 1990, quando Poulsen interceptou todas as linhas telefônicas da estação de rádio KIIS-FM, vencendo assim um concurso realizado pela emissora da Califórnia. O prêmio era um Porsche para o 102º ouvinte que telefonasse. Poulsen garantiu seu carro, mas passou 51 meses na prisão. Hoje ele é diretor do site Security Focus e editor da Wired.

## ● Onel de Guzman



Criador do famoso vírus "I love you", que era enviado por e-mail com um arquivo anexo chamado "Love-the-letter-for-you". Após a execução, o vírus fazia com que a mensagem fosse enviada para todos os contatos da vítima, e além de se retransmitir, o vírus subscrevia alguns arquivos e infectava vários outros, fazendo com que o malware fosse executado toda vez que a pessoa tentasse abrir um arquivo MP3, por exemplo. Estima-se que o "I love you" tenha sido enviado a mais de 84 milhões de pessoas, causando um prejuízo total de \$8,7 bilhões.

# ● Jonathan James



Foi o primeiro adolescente a ser preso por crimes digitais nos Estados Unidos, em 1999. Ele invadiu os computadores do Departamento de Defesa dos Estados Unidos e da NASA, aos 15 anos de idade. James suicidou-se em maio de 2008, e junto com o corpo foi encontrada uma carta com 5 páginas, justificando que ele não acreditava mais no sistema judiciário. Isso porque ele estava sendo investigado pelo Serviço Secreto por ter ligação - ao qual ele negava - a um grande roubo de dados de clientes de várias lojas virtuais norte-americanas em 2007.

# ● Kevin Mitnick



O mais famoso hacker da história. Em 1990, Kevin Mitnick invadiu vários computadores de operadoras de telefonia e provedores de internet, além de enganar o FBI e se transformar em um dos cibercriminosos mais procurados da internet (história que chegou até a virar filme). Em 1995 ele foi preso, sendo liberado 5 anos depois após pagar fiança, mas nos primeiros três anos de liberdade não pode conectar-se a internet. Hoje, Mitnick é um consultor de segurança digital, tendo participado inclusive do evento Campus Party 2010 no Brasil.

# FIREWALL



Firewall é um termo inglês que em português significa literalmente parede de fogo e designa uma medida de segurança implementada com o objetivo de limitar ou impedir o acesso de terceiros a uma determinada rede ligada à Internet. A implementação deste tipo de mecanismos pode envolver ferramentas de hardware ou de software ou mesmo uma combinação de ambos, os quais, no limite, podem impedir qualquer ligação entre a rede interna e outras redes externas

# DICAS DE SEGURANÇA



- Cuidado ao abrir e-mails com qualquer tipo de anexo! Normalmente estes anexos ou links dão acesso ao vírus e os liberam.
- Ao acessar um arquivo possivelmente vírus, ele solicitará o download e terá uma das seguintes extensões:
  - Exe;
  - Scr;
  - Bat;
  - Pif;
  - Vbs.

# DICAS DE SEGURANÇA



- Mantenha o seu sistema sempre atualizado;
- Tenha um anti-vírus ativo;
- Tenha um ou mais anti-spyware ativos

# Cookies e Arquivos temporários



**Cookies** são pequenos programas instalados nos HDs por empresas de sites. O objetivo desses cookies é enviar para empresa quais partes do site mais interessa ao usuário e quais sites o usuário mais visita (espécie de espionagem para verificar o tipo de cliente)

# LIMPEZA E DESFRAGMENTAÇÃO DE DISCOS



**Limpeza**, consiste em retirar os arquivos temporários e os cookies do computador.

O próprio Windows oferece recursos para fazer a limpeza. Para acessá-lo é só clicar em Iniciar – Programas, ou Todos os Programas – Acessórios – Ferramentas do Sistema – Limpeza de disco.

# LIMPEZA E DESFRAGMENTAÇÃO DE DISCOS



**Desfragmentação** consiste em desfragmentar arquivos ou programas. Quando utilizamos um arquivos várias vezes aos poucos ele se desfragmenta no nosso HD. Além disso, muitas vezes apagamos e colocamos programas ou arquivos no nosso computador. Quando apagamos deixamos espaços vazios no HD, fazendo que outro arquivo ocupe aquele espaço, quando criado, e se não há espaço o suficiente para se guardar o arquivo ele se completa em outra parte do HD fragmentando o arquivo.

# LIMPEZA E DESFRAGMENTAÇÃO DE DISCOS



É claro que existe programas que fazem estes serviços no nosso computador. Muitas vezes melhor que os próprios recursos do Windows por terem mais recursos neles. Apresentarei os melhores programas para estas funções: o CClear (para limpeza do computador) e o Disk-Defrag (Para desfragmentação do HD)



## 1.3.1 Cifras de Substituição

Nas cifras de substituição cada grupo de letras é **substituído** por outro grupo de letras.

- Substituindo as letras da palavra "**paz**" pela correspondente resultaria em "**HQN**".

|   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m |
| Q | W | E | R | T | Y | U | I | O | P | A | S | D |
| n | o | p | q | r | s | t | u | v | x | y | z | w |
| F | G | H | J | K | L | Z | X | C | V | B | N | M |

Figura. Cifras de substituição



## 1.3.2 Cifras de Transposição

As cifras de transposição utilizam o princípio de mudança da **ordem** das letras da mensagem a ser enviada.

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| b | r | a | s | i | l |
| 2 | 5 | 1 | 6 | 3 | 4 |
| m | i | n | h | a | l |
| i | n | d | a | o | n |
| d | e | t | e | e | n |
| c | o | n | t | r | o |

Figura. Cifras de transposição

- No exemplo acima, a **chave** serve de apoio para enumerar as colunas na ordem alfabética crescente das letras.
- O texto é lido na vertical, resultando em: **"ndtnmidcaorerlnnoineohaet"**

Teste de raciocínio. Identifique os ditados populares abaixo pelos emotions. Se acertar pelo menos um, compartilhe



**Este problema pode ser resolvido por uma criança em até 10 minutos, por programadores em até 1 hora e por pessoas de cursos superiores em... bem... tente descobrir!**

|          |            |
|----------|------------|
| 8809 = 6 | 5555 = 0   |
| 7111 = 0 | 8193 = 3   |
| 2172 = 0 | 8096 = 5   |
| 6666 = 4 | 1012 = 1   |
| 1111 = 0 | 7777 = 0   |
| 3213 = 0 | 9999 = 4   |
| 7662 = 2 | 7756 = 1   |
| 9313 = 1 | 6855 = 3   |
| 0000 = 4 | 9881 = 5   |
| 2222 = 0 | 5531 = 0   |
| 3333 = 0 | 2581 = ??? |

# INTRODUÇÃO



Uma informação é um arranjo de dados (nomes, palavras, números, sons, imagens) capazes de dar forma ou sentido a algo do interesse de alguém.

**Dados + Contexto => Informação**

# A complexa malha de Comunicação Mundial

*O desenvolvimento e a gestão dos negócios apóiam-se, invariavelmente, em conexões estabelecidas em três níveis: **internet, intranets e extranets.***

- **internet:** *suporte às atividades de e-business e e-commerce, integrando a organização no mercado global.*
- **extranet:** *rede proprietária ligando a empresa a entidades externas mais próximas.*
- **intranet:** *sistema interno de comunicação e informática, operando nos moldes da internet no apoio a operação e gerência.*



**INTERNET**

**EXECUTIVO DA EMPRESA**



**EXTRANET**

**EXTRANET**

**EXTRANET**

**EXTRANET**



**FIREWALL**



**FIREWALL**



**FILIAL 1 - INTRANET**



**MATRIZ - INTRANET**



**FIREWALL**



**FILIAL 2 - INTRANET**

Professora: Rosana Barbosa

# ***e-business***



*é o processo em que se estabelece  
ligação  
eletrônica entre uma organização, seus  
clientes, seus fornecedores e demais  
elementos de seu relacionamento, com  
o objetivo de obter maiores ganhos nos  
negócios.*



Clients



Online catalogs



Sales



Auctions



Payments



Web Factory



E-Mail Factory



My Company



# ***e-commerce***



*é o processo de compra e venda de bens e*

*serviços pela internet. Pode ser:*

***B2B – estabelecidos entre empresas***

***B2C – estabelecido entre empresa e cidadão***

***B2G – estabelecido entre empresa e governo***

***G2G – estabelecido entre governos***





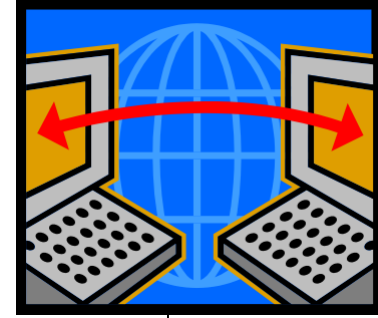
***World Wide Web (WWW ou 3W ou Web) - Um dos muitos serviços de comunicação disponibilizados na internet.***

***Site (Website) - um sítio ou lugar na Web; em principio, é uma composição de páginas interligadas, isto é, o total de uma comunicação ou Publicação.***

***Homepage – página inicial de um site.***

***Frequentemente, no entanto, utilizam-se site e homepage como termos sinônimos, equivalentes.***

# Introdução



- Redes de Computadores e a Segurança
  - As corporações (empresas, governos e escolas) estão cada vez mais dependentes de seus sistemas – exigem informações compartilhadas;
  - Uso de informações sigilosas (comércio eletrônico)
  - Novas tecnologias (por exemplo, redes sem fio)



Necessidade de se manter a  
Segurança das Informações

# As preocupações crescem....



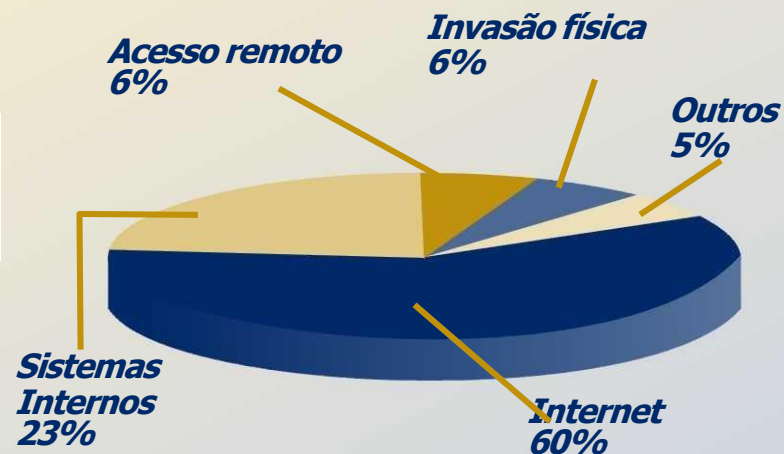
- Aumento do uso da Internet
- Aumento do registro dos incidentes de segurança (intrusos e funcionários insatisfeitos)
- Numerosos relatos de vulnerabilidades de softwares (inclusive os de segurança)
- Proteção física é dificilmente concretizada

Segurança de Redes é uma  
tarefa árdua e complexa !

# 9ª Pesquisa Nacional de Segurança da Informação



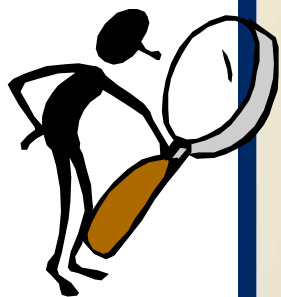
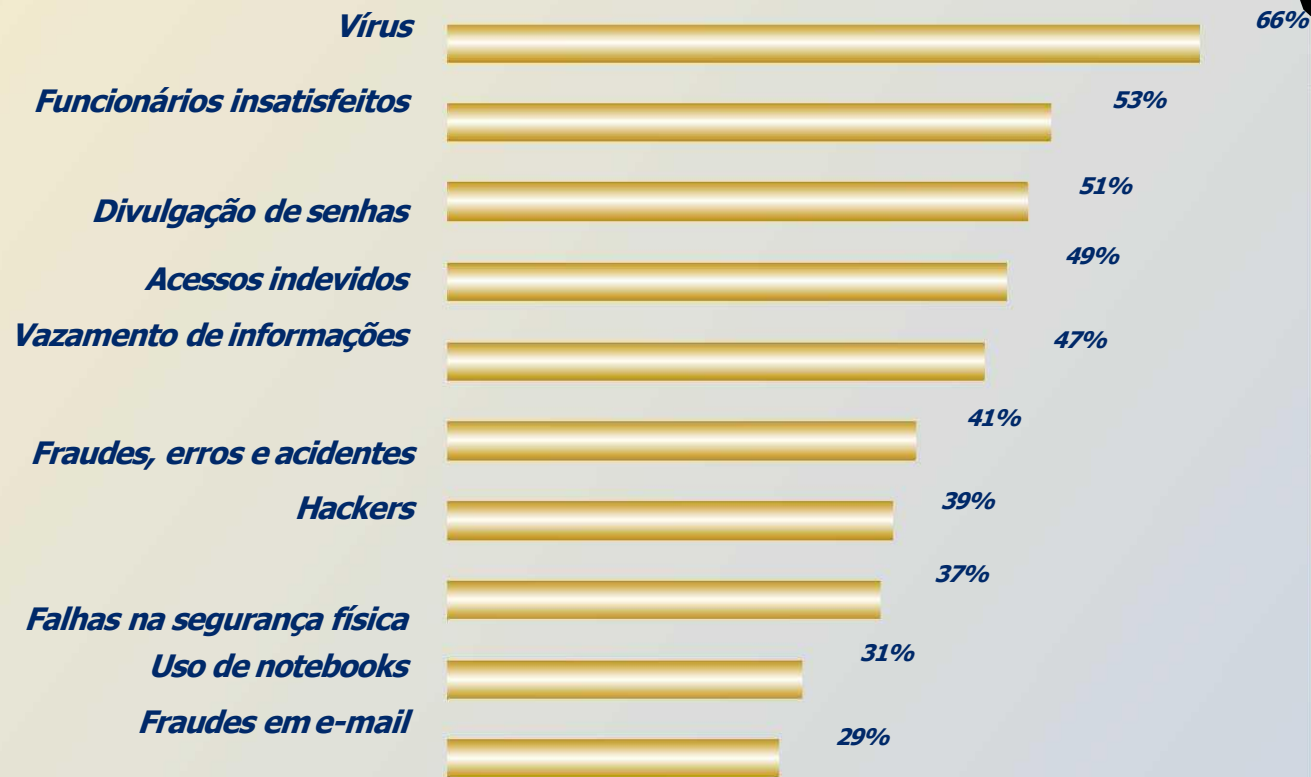
**PRINCIPAIS PONTOS DE INVASÃO**



# 9ª Pesquisa Nacional de Segurança da Informação



## PRINCIPAIS AMEAÇAS À SEGURANÇA DA INFORMAÇÃO

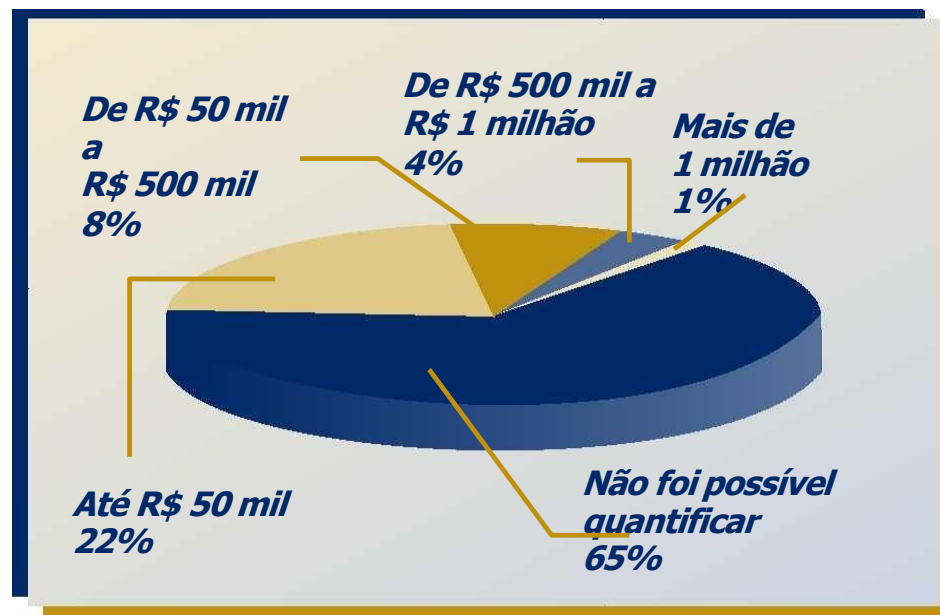


# 9ª Pesquisa Nacional de Segurança da Informação

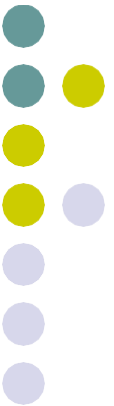


- > 35% das empresas no Brasil tiveram perdas financeiras
- > 22% das empresas acima registraram perdas de até R\$ 50 mil, 8% entre R\$ 50 mil e R\$ 500 mil e 4% de R\$ 500 mil a R\$ 1 milhão
- > 65% não conseguem quantificar o valor dos prejuízos

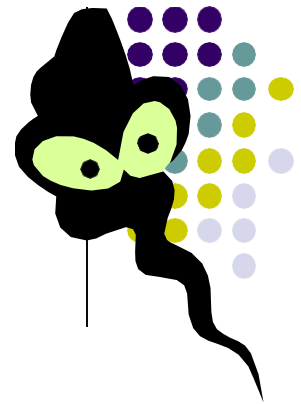
## PREJUÍZOS CONTABILIZADOS



# Aplicativos Maliciosos



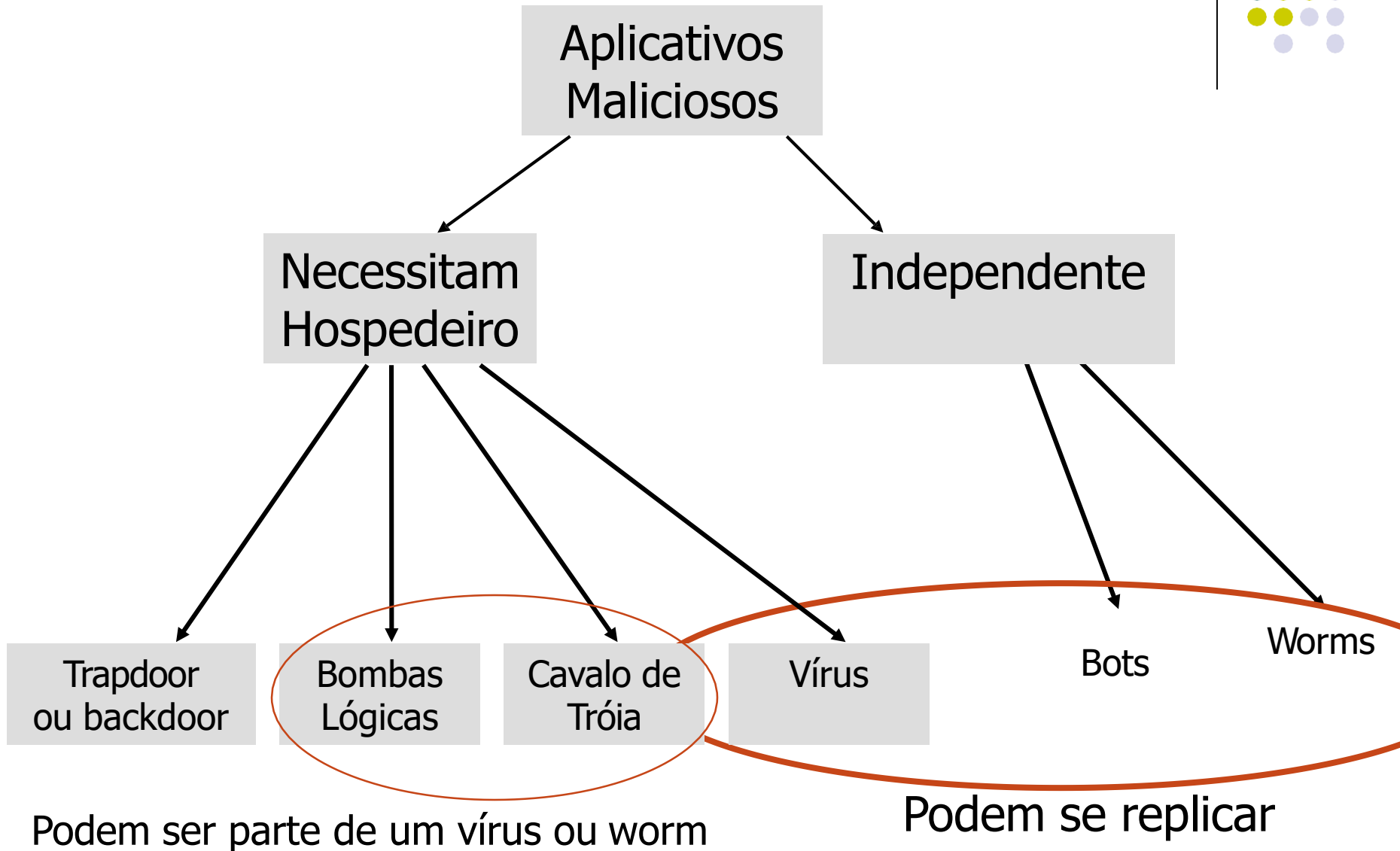
# Definição



Malware = Malicious Software

- Aplicativos/programas que exploram vulnerabilidades nos sistemas computacionais
- Podem ser divididos em duas categorias
  - Os que precisam de um aplicativo hospedeiro
  - Os que são independentes
- E também são diferenciados por poderem ou não se replicar

# Taxonomia dos *Malwares*





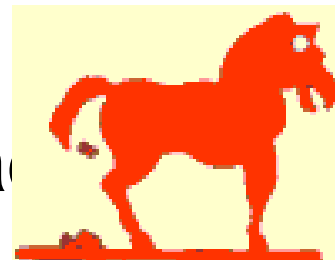
# Bombas Lógicas

- Um dos mais velhos aplicativos maliciosos, precedendo os vírus e *worms*
- Código embutido em programas legítimos que quando certas condições forem atingidas ele “explode”
  - Data específica
  - presença ou falta de arquivos
  - determinado usuário que esteja rodando a aplicação
- Quando é disparada, pode apagar e alterar ou remover dados ou arquivos inteiros, causar uma pane na máquina ou algum outro dano



# Cavalo de Tróia (*trojan horse*)

- Programa que além de executar as funções para as quais foi projetado, também executa outras funções maliciosas sem o conhecimento do usuário
- Funções maliciosas que podem ser executadas
  - alteração ou destruição de arquivos
  - furto de senhas e outras informações sensíveis
  - inclusão de backdoors, para permitir que um atacante tenha total controle sobre o computador
- Arquivo único que necessita ser executado





# Cavalo de Tróia

- Ações semelhantes a dos Vírus e *Worms*
- Distingue-se por não se replicar, infectar outros arquivos, ou propagar cópias de si mesmo automaticamente
- Fotos, arquivos de música, protetores de telas e jogos
- Enviados por email ou disponíveis em *sites* da Internet

# CAVALO DE TRÓIA



# Vírus



- É um aplicativo que consegue “infectar” outros programas e arquivos, modificando-os.
- A modificação inclui uma cópia do vírus, o qual poderá infectar outros aplicativos.
- Vírus típicos, tomam o controle temporário do sistema operacional, incluindo suas cópias em novos aplicativos
- A contaminação entre máquinas pode ser realizada através de dispositivos removíveis (pen-drives/ CDs) ou pela rede (abrir arquivos anexos aos e-mails, abrir arquivos Word, Excel, abrir arquivos em outros computadores) – Arquivos precisam ser executados



1. Enquanto você navega na internet, qual das opções abaixo **não aumentará** a segurança?
  - A. Instalar as atualizações de segurança do navegador.
  - B. Verificar o link antes de acessá-lo.
  - C. Acessar somente sites com “http://”.
  - D. Estar com antivírus atualizado e funcionando.

2. Você está trabalhando e alguém da TI liga solicitando sua senha para realizar uma configuração **urgente**. Essa solicitação não foi realizada. O que deve ser feito?

- A. Repassar a sua senha por telefone, pois é uma solicitação urgente.
- B. Repassar a sua senha, mas pedindo para redefini-la depois que usar.
- C. Não repassar a senha, já que um colaborador da TI não solicitaria essa informação, pois ela é pessoal e intransferível.
- D. Questionar sobre a solicitação repentina, mas acaba repassando a senha, pois se trata de alguém da TI.

3. Qual das seguintes opções é um exemplo de um comportamento seguro de um Agente da Segurança da Informação Positivo Tecnologia?



- A. Deixar seu computador desbloqueado ao sair da mesa.
- B. Denunciar um e-mail suspeito para o time de Segurança da Informação Corporativo.
- C. Clicar em links de e-mails com remetentes desconhecidos.
- D. Instalar softwares piratas.

## 4. Este e-mail provavelmente é um phishing, por quê?



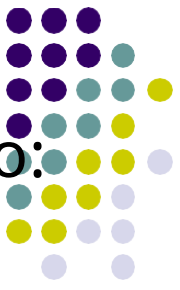
- A. Contém um link.
- B. Foi enviado por uma “equipe de segurança”.
- C. O e-mail foi recebido fora do horário de expediente.
- D. Está pedindo uma ação urgente, contém erros de ortografia e o domínio do remetente não é o oficial.

5. Qual prática é a mais segura ao criar suas senhas?



- A. A senha deve ser comprida, mas com palavras fáceis e sequenciais.
- B. Usar informações pessoais, como por exemplo, nome e data nascimento que seja fácil de lembrar.
- C. Usar senhas complexas e salvar no bloco de notas.
- D. Usar somente senhas complexas, que tenham caracteres especiais, letras maiúsculas/minúsculas, numerais.

6. Algumas das atitudes abaixo são consideradas boas práticas a serem tomadas em suas estações de trabalho:



**1. Deixar lembretes com senhas e informações sigilosas na mesa.**

**2. Imprimir documentos só quando necessário**

**3. Bloquear o computador sempre que se ausentar.**

**4. Deixar bens e documentos confidenciais sobre a mesa.**

**5. Deixar blocos de notas com suas senhas armazenadas na área de trabalho do seu computador.**

Selecione a alternativa correta:

- V – V – F – F – V.
- F – V – V – F – F.
- V – F – F – V – F.
- F – F – V – V – F.



10. Você está navegando na internet, aparece um anúncio de uma promoção de queima de estoque de uma loja conhecida. Ao clicar no link do anúncio há um redirecionamento para um site diferente do qual está habituado. O que fazer?

- A. Informo meus dados para continuar, pois não posso perder a promoção.
- B. Acho estranho, mas acabo inserindo meus dados para continuar.
- C. Percebo a fraude, fecho o site e procuro o endereço oficial da loja para verificar a veracidade da promoção.
- D. Acesso o site com meus dados e realizo uma compra.