SEGURANÇA EM TI

Tiago Alves de Oliveira

toliveira@divinopolisuemg.com.br

Segurança da informação

- O que é informação?

  Ativo que tem valor para a organização;

  É o bem ativo mais valioso da organização?

- Onde está a informação?

  Papel;

  Banco de dados...

- Por que proporcionar segurança para a informação?

Segurança da informação

- Características básicas da segurança da informação:

  Confidencialidade

  - A informação é acessada somente por pessoas autorizadas?

  Integridade

  - Há garantia de que a informação acessada não foi alterada?

  Disponibilidade

  - A informação está acessível no momento necessário?

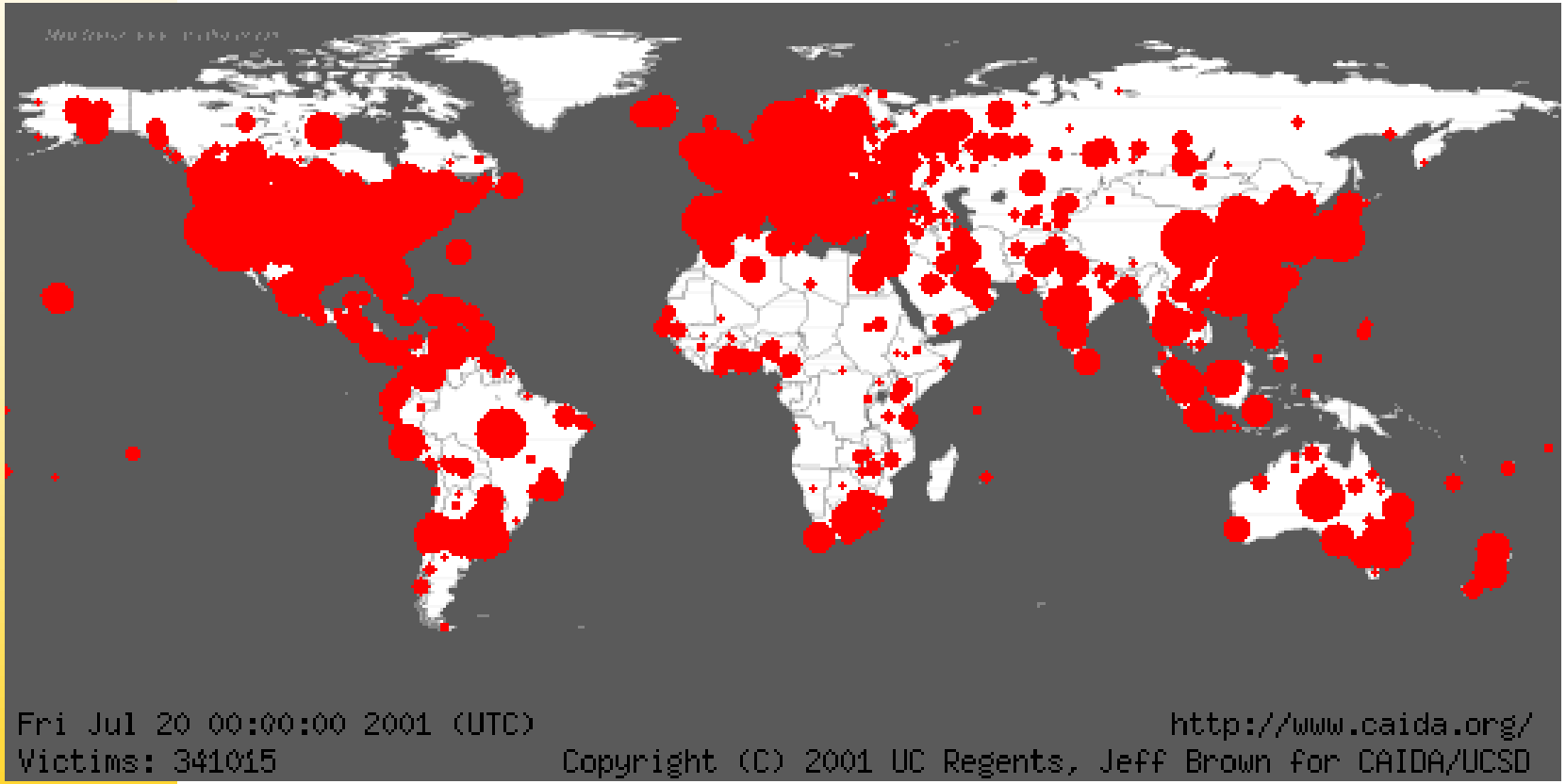
Segurança da Informação

- Áreas da segurança da informação:

  Segurança física
  Segurança lógica
  Segurança de pessoas
  Segurança de computadores
  Segurança de redes
  Segurança de aplicativos

Ano de 2001

- *Worm* Code Red



Expansão do *worm* Code Red em 14 horas
Fonte: http://www.caida.org/research/security/code-red/coderedv2_analysis.xml

Principal

Princípios básicos de segurança

1) Menor privilégio (least privilege)

Princípio fundamental. Define que cada objeto (usuário, administrador, programa...) deve possuir apenas o mínimo de privilégio

2) Defesa em profundidade (defense in depth)

Não se deve confiar em um único mecanismo de segurança; deve-se sempre utilizar defesas redundantes

3) Gargalo (choke point)

Obriga intrusos a usar um canal estreito que pode ser monitorado e controlado

Princípios básicos de segurança

4) Falha segura (fail-safe stance)

Quando o sistema de segurança falha, deve falhar de tal forma que bloqueie o acesso de um invasor, em vez de deixá-lo entrar

5) Participação universal (universal participation)

O sistema de segurança deve envolver todos os objetos (pessoas)

6) Diversidade de defesa (diversity of defense)

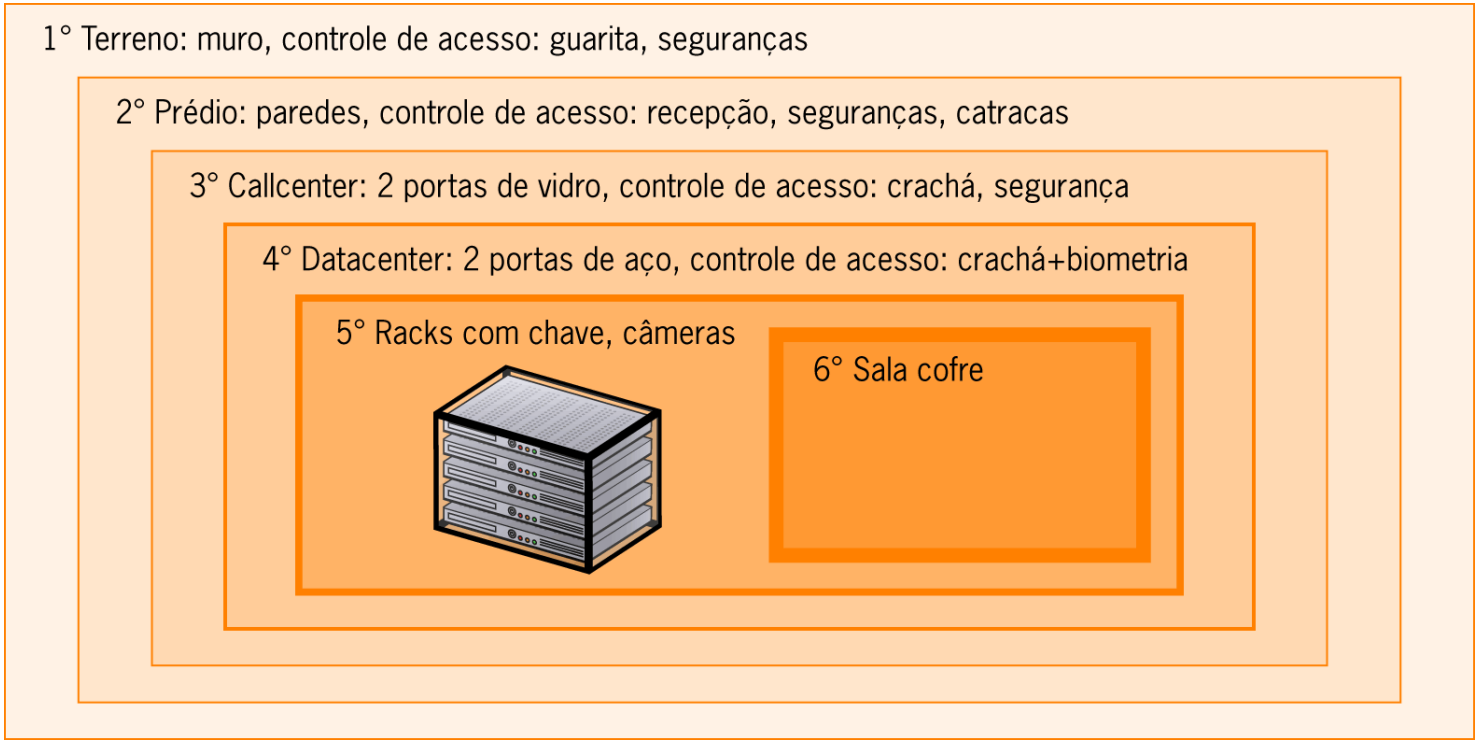
Não é um princípio geral. Afirma que o uso de sistemas diferentes torna o sistema (como um todo) mais seguro

Segurança física

- Segurança externa e de entrada
- Segurança da sala de equipamentos
- Segurança dos equipamentos
- Redundância
- Segurança no fornecimento de energia
- Salvaguarda (*backup*)
- Descarte da Informação

Segurança física

- Em nível físico: formação de perímetros e aplicação de três princípios básicos de segurança: defesa em profundidade, gargalo e diversidade de defesa.



Biometria

- Impressão Digital (Identix TouchSafe Personal)
- Reconhecimento Facial (Miros TrueFace)
- Reconhecimento de Voz (VeriVoice)
- Identificação da Iris (IrisScan)
- Identificação de Retina
- Reconhecimento da Geometria da Mão
- Reconhecimento da Assinatura Manuscrita
- Reconhecimento da Dinâmica de Digitação
- Multi-reconhecimento Biométrico

Segurança física

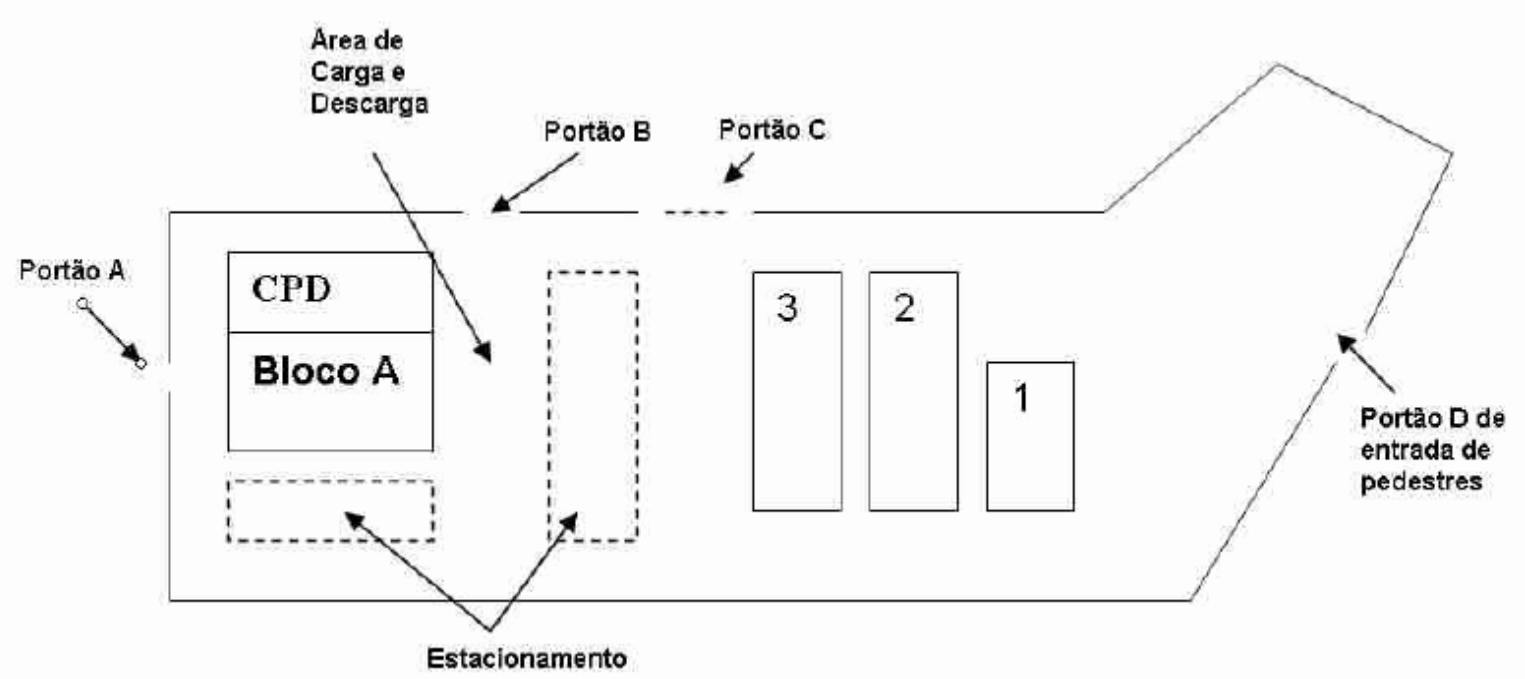
- Os equipamentos de rede e servidores devem estar em uma sala segura
- Os equipamentos devem ser protegidos contra acessos indevidos no seu console, através de periféricos como teclado, *mouse* e monitor
- Travas para disquetes ou CDs são recomendadas
- Os equipamentos devem ser protegidos contra acessos indevidos ao interior da máquina
- Notebooks ?

Gabinete de computador com porta e chave

Tranca para gabinete de computador

Principal

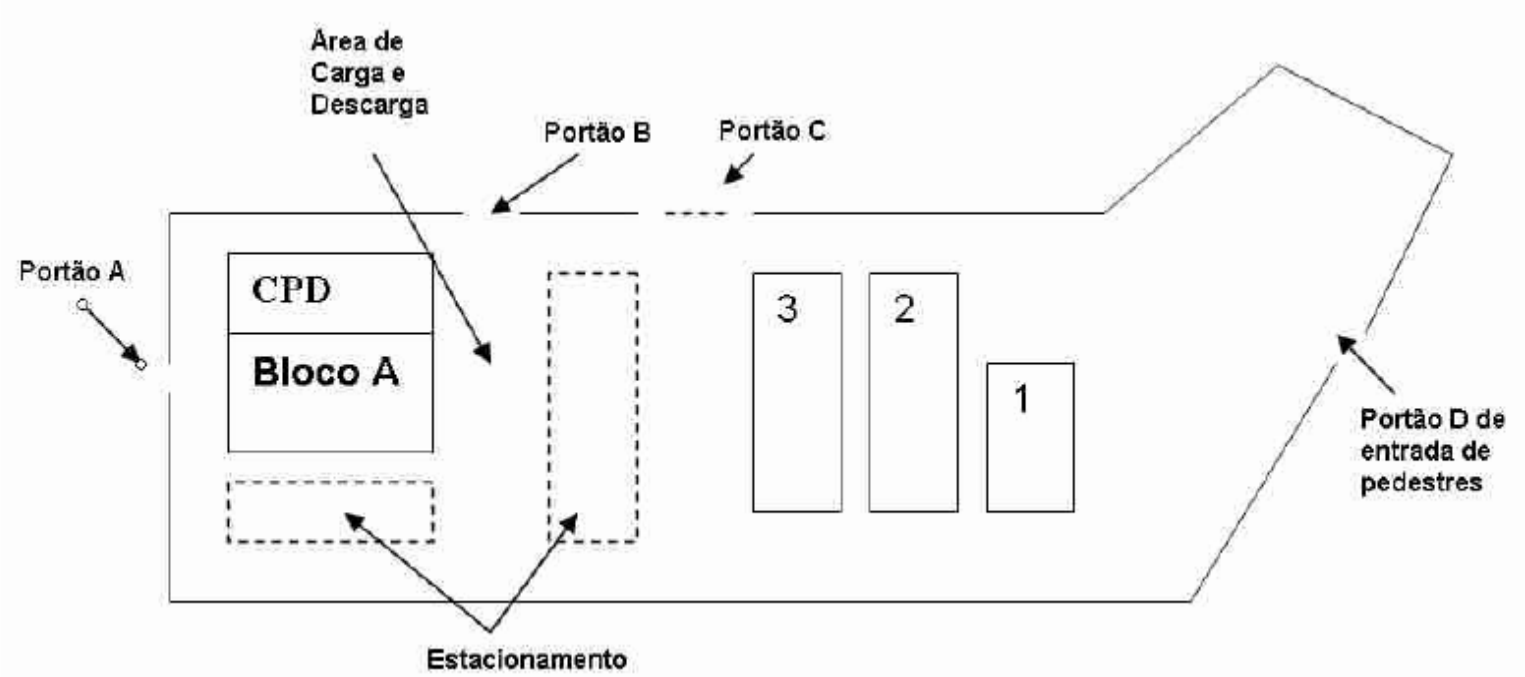
Estudo de caso



O desenho acima mostra o site de uma empresa que abrigará um novo CPD.
O terreno é cercado por grades (aprox. 2 metros), com 4 portões:
Portão A: entrada para o bloco A
Portão B: entrada de funcionários e de caminhões para carga e descarga
Portão C: atualmente desativado (portão grande)
Portão D: entrada de pedestres(portão pequeno)

Principal

Estudo de caso



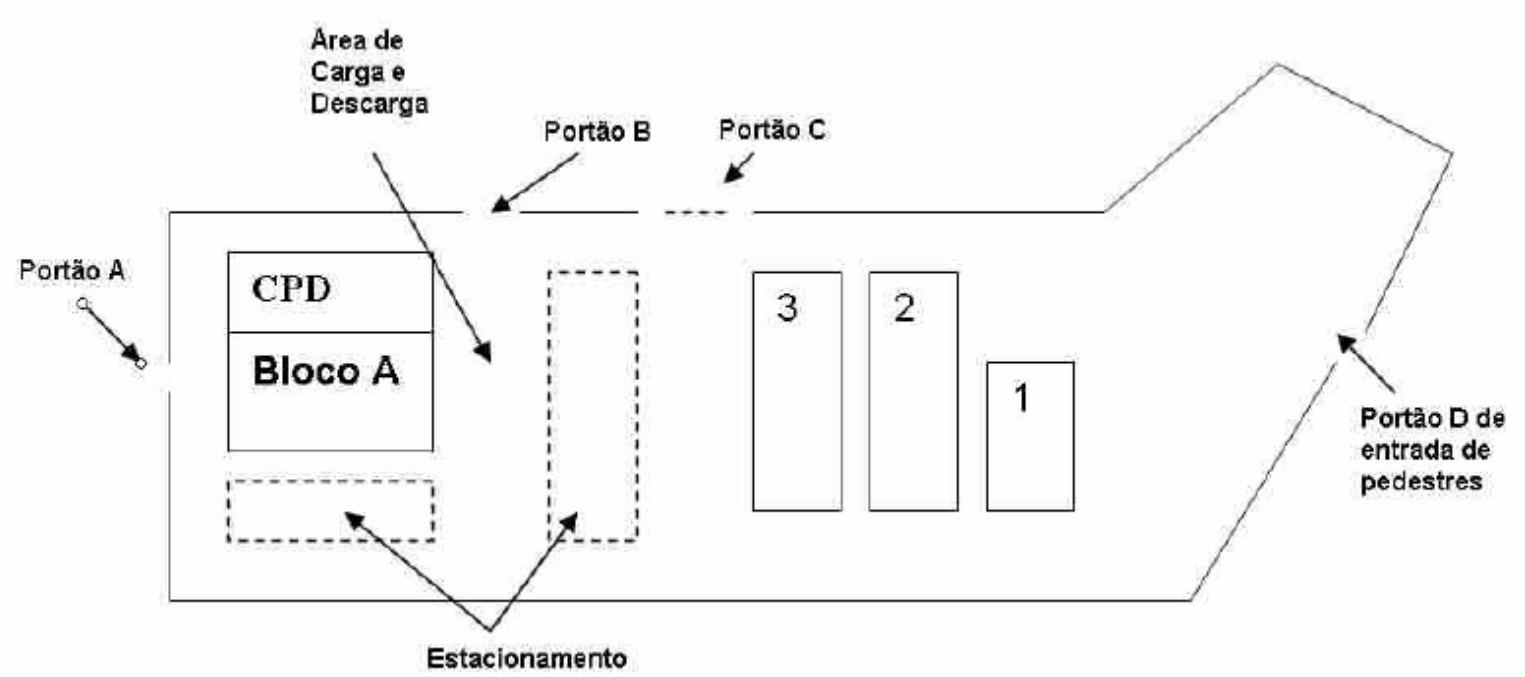
O terreno contém 4 construções:

Bloco A:

No subsolo, há 3 depósitos distintos:

1. papelaria e material de expediente;
2. móveis usados;
3. equipamentos de informática reutilizável.

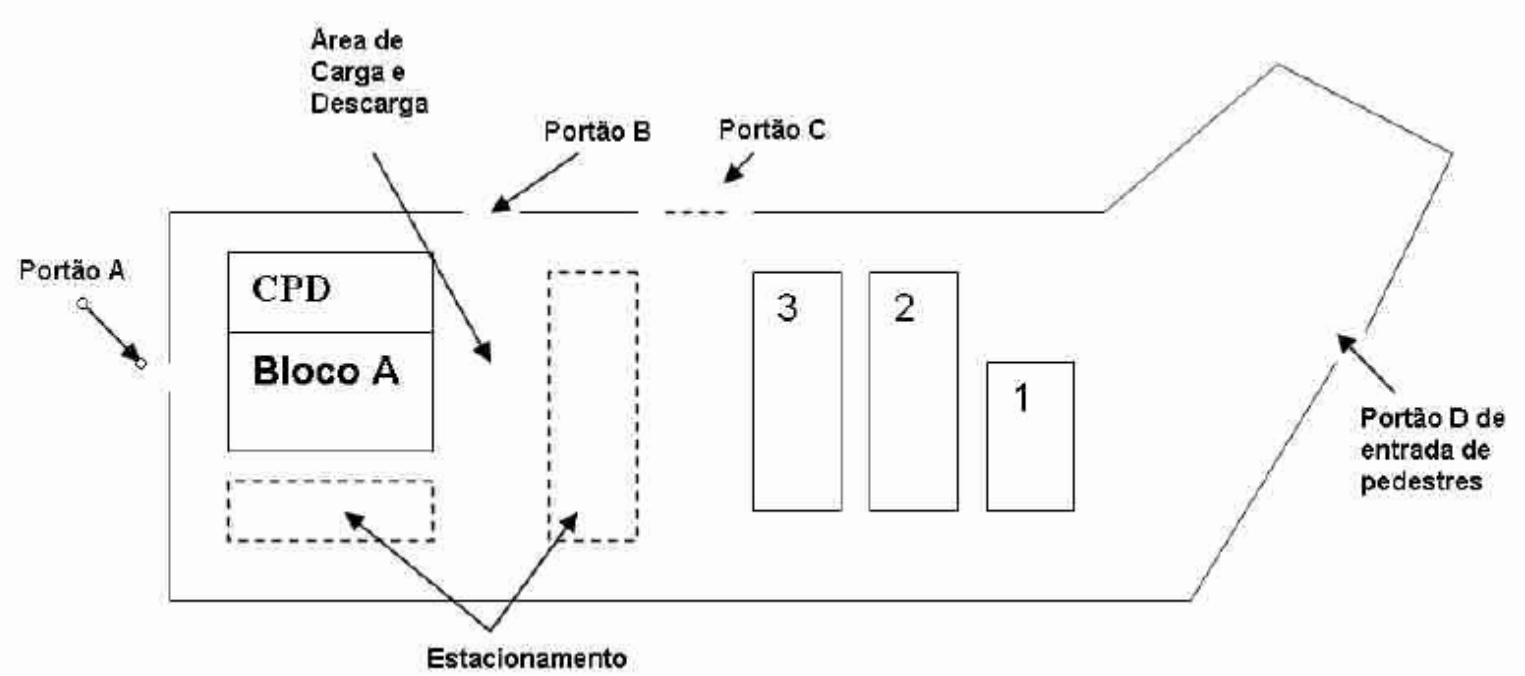
Estudo de caso



No térreo funcionam uma gráfica, um estoque de atacado e a rampa de carga e descarga.

No primeiro andar funcionará o CPD e um novo setor com um grande volume de cheques. Separados do CPD por uma parede corta-fogo estarão a gráfica plana, o escritório e o laboratório da gráfica, que contém materiais altamente inflamáveis.

Estudo de caso

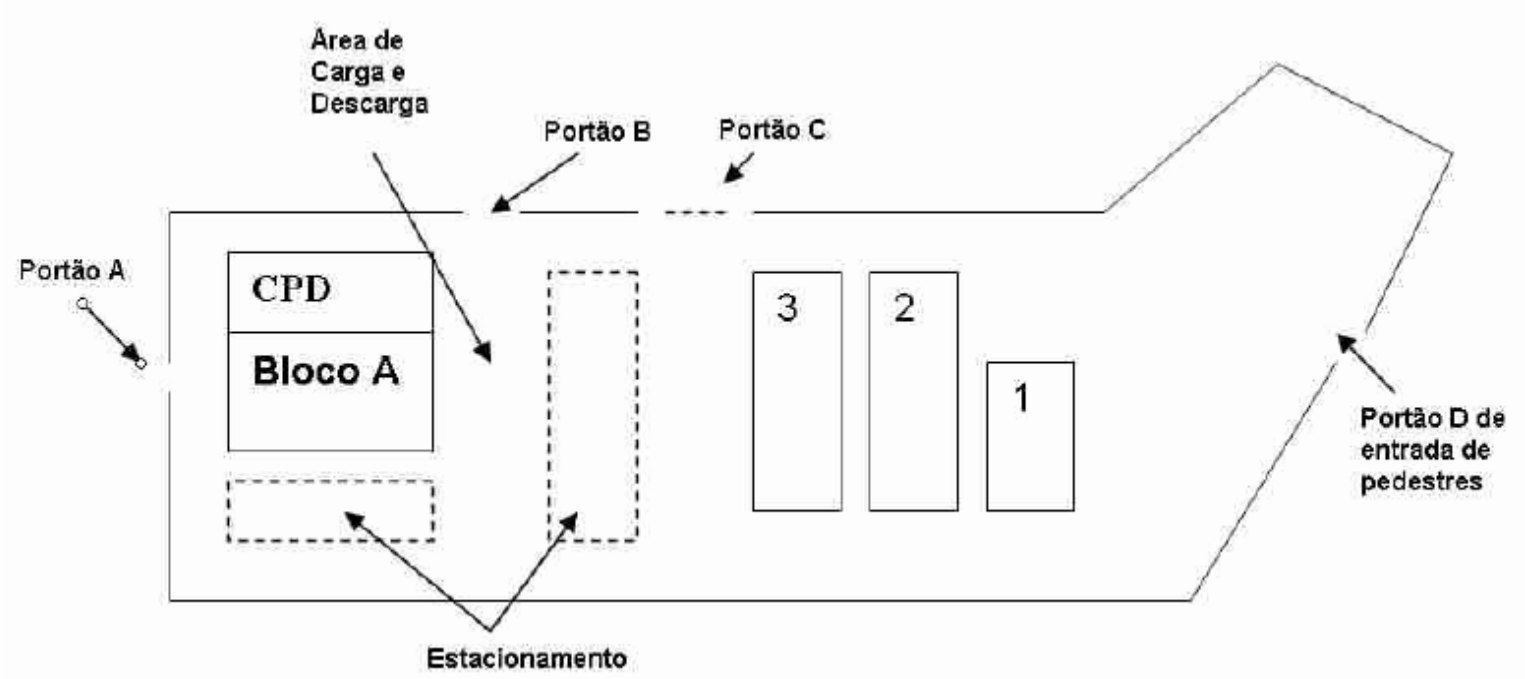


Existem 2 entradas para o CPD. A principal, pelo portão A e uma outra pela área de carga e descarga.

Pavilhão 1: documentos de microfilmagem e papéis
Pavilhão 2: Setorial de transporte, estoque de papel da gráfica e lanchonete
Pavilhão 3: móveis e equipamentos obsoletos

Principal

Estudo de caso



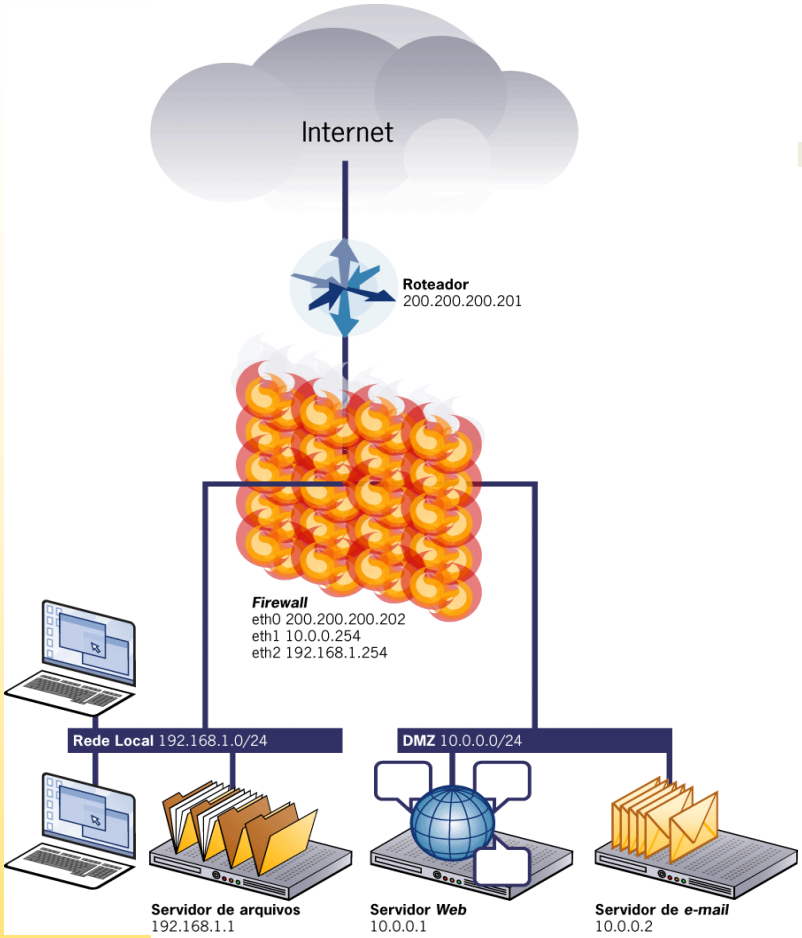
Tendo em vista a segurança física:

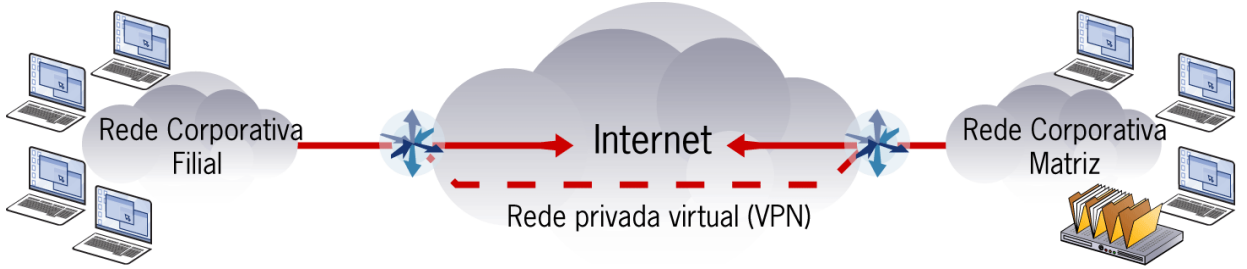
1. Quais são os riscos com relação a acesso, incêndio, inundação, etc?
2. Quais ações/soluções vocês recomendariam?

Segurança lógica

- *Firewall*
- Detector de intruso
- Rede virtual privada
- Autenticação, autorização e auditoria

Segurança lógica





Principal

Segurança lógica

- Autenticação:

  Identificação:

  - Via algo que você sabe
  - Via algo que você tem
  - Via algo que você é

- Autorização :

  Perfil

- Auditoria

  Quem fez o quê, quando, aonde?

Morais da Segurança

- As portas dos fundos são tão boas quanto às portas da frente.

Principal

Morais da Segurança

- Uma corrente é tão forte quanto o seu elo mais fraco.

Morais da Segurança

- Um invasor não tenta transpor as barreiras encontradas, ele vai ao redor delas buscando o ponto mais vulnerável.

10 Erros mais Comuns de Segurança

1) A não alteração das senhas de todos os dispositivos da rede.

Problema facilmente resolvido com a troca de senhas ″Padrão″ por senhas não usuais periodicamente em todos os dispositivos que possuam um *IP*.

2)**Compartilhamento de senhas.**

Esse péssimo hábito de colocar a mesma senha para vários dispositivos. Isso dever se alterado por meio de um processo que garanta que as senhas não sejam compartilhadas e sejam trocadas regularmente.

3)Falha no SQL.

Quase 80% dos ataques são por meio da inserção de um codigo *SQL* em formulários *Web* para atingir banco de dados com essa linguagem. Para evitar isso basta ativer ″*firewall*″ que filtram as entradas dos formulários e restringir o acesso de dispositivos que não sejam essenciais aos servidores. Assim a empresa previne o acesso através de um erro de *SQL*.

10 Erros mais Comuns de Segurança

4) **Configuração na lista de controle de Acesso, má revisada ou autorizada.**

Para simplificar ainda mais a solução desse problema é segmentar a rede com uma lista de controle de acesso. Mais cuidado, caso o *hacker* consiga entrar na rede de um dos seus parceiros e seu servidor não tiver adequadamente protegido, seus dados estarão disponíveis.

5) **Uso de acesso remoto ou *softwares* de gerenciamento sem segurança.**

Programas como o *VNC* são caminhos de entrada de *hackers*. E a única forma é o profissional fazer uma varredura externa de todo o endereço IP procurando por tráfego desse tipo de *software*. Encontrando, deve-se tomar medidas extras de segurança, como certificados que se juntem as senhas.

6) **Busca de vulnerabilidade básica em aplicações não-críticas.** Para garantir testes devem ser feitos em todas as aplicações abrangendo pelo menus as vulnerabilidades básicas, mais lembre-se o *hacker* não escolhe o ataque pelas aplicações críticas mais pela ordem do que é mais fácil.

10 Erros mais Comuns de Segurança

7)Falta de proteção contra *Malwares*.

Malwares instalados nos servidores são responsáveis por cerca de 40% de todas as brechas em segurança. Esse tipo de proteção roda somente em servidores críticos e o ideal é fazer uma varredura em toda a rede.

8)Falha em proibir tráfego externo em roteadores.

Para evitar a infiltração de *Malwares* e o uso dos mesmos por *hackers* basta a aplicação de uma lista de controle de acessos, bloqueando assim o servidor de enviar dados que não deveria. **ex.** um servidor de e-mails de enviar somente *e-mails* e para sua lista de contatos.

10 Erros mais Comuns de Segurança

9) Falta de conhecimento de onde dados críticos estão armazenados.

A maioria das Empresas acreditam saber onde estão os dados como CPFs, cartões de crédito, adotando o nível mais alto nesses servidores, mais se esquecem que em outros departamentos podem existir *backups* e esses são chamados de servidores secundários. Normalmente são esses servidores secundários que vazam os dados.

10) Indústria de pagamentos – Falta de atenção aos padrões de segurança.

A indústria financeira tem várias regras que seguidas com rigor são muito eficazes para garantir a segurança dos pagamentos.

Motivação

- O que leva uma pessoa a invadir um sistema?

  Impunidade

  Delinqüência

  Tentativa de chamar a atenção

  Vingança

  Compensação financeira

  Espionagem

Ameaças recentes

Fraude *on-line*:

- Visa seqüestro de dados bancários e informações úteis ao malfeitor
- Aborda em larga escala usuários via *e-mail*
- Usa assunto atrativos como disfarce
- Induz a vítima a fornecer dados sigilosos
- Instala programa que rouba informações no computador

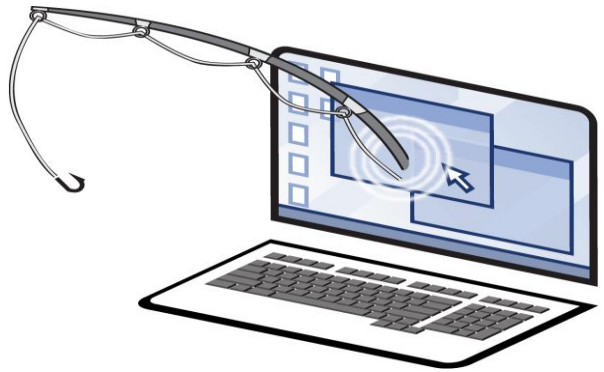
Phishing Scam

Formas atuais

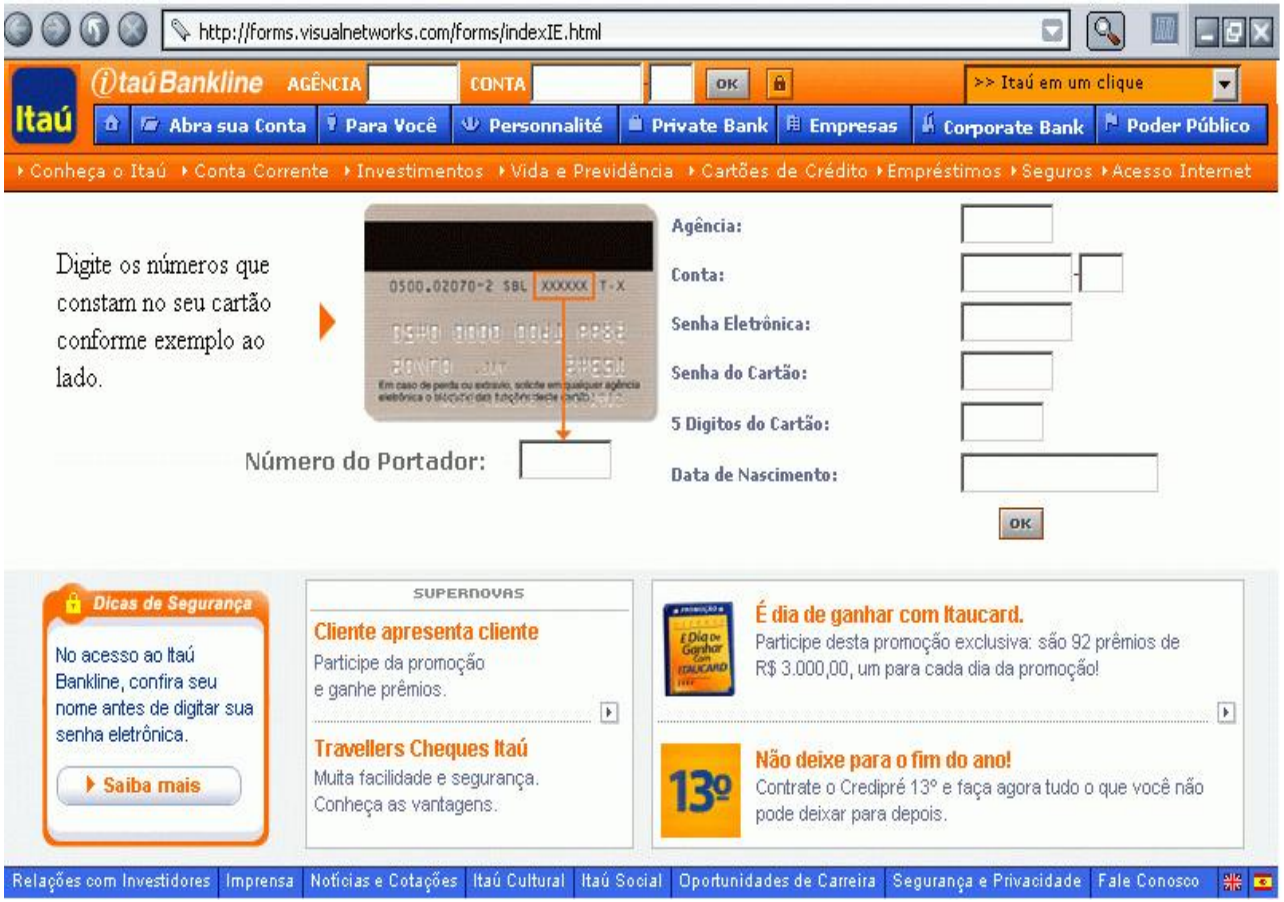
- *Link* para programa malicioso
- Página falsificada de comércio eletrônico ou *internet banking*
- *E-mail* contendo formulário
- Mensagens Maliciosas

Cuidados ao usar comércio eletrônico ou *internet banking*

Proteção anti-*phishing*

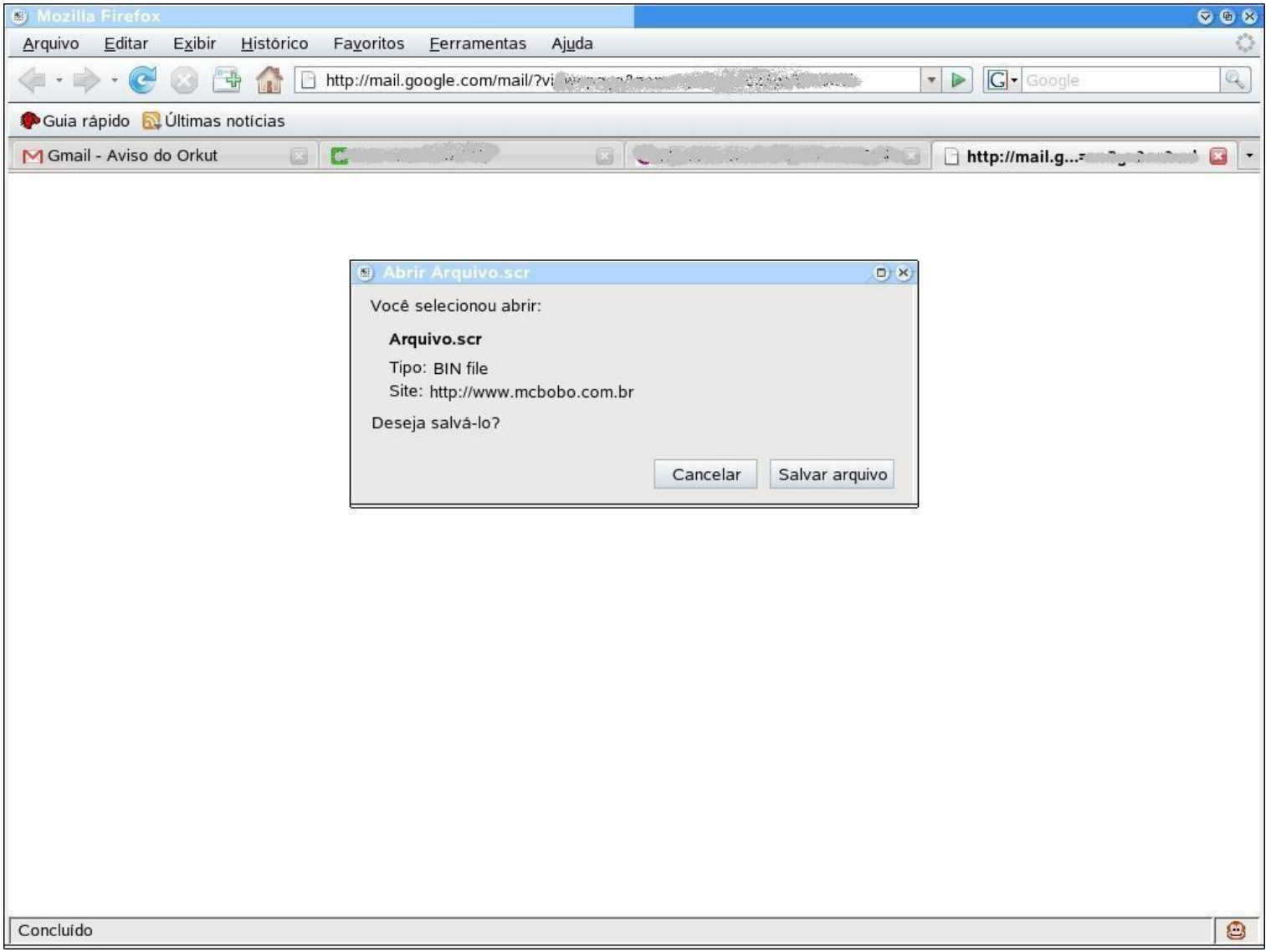


Phishing Scam

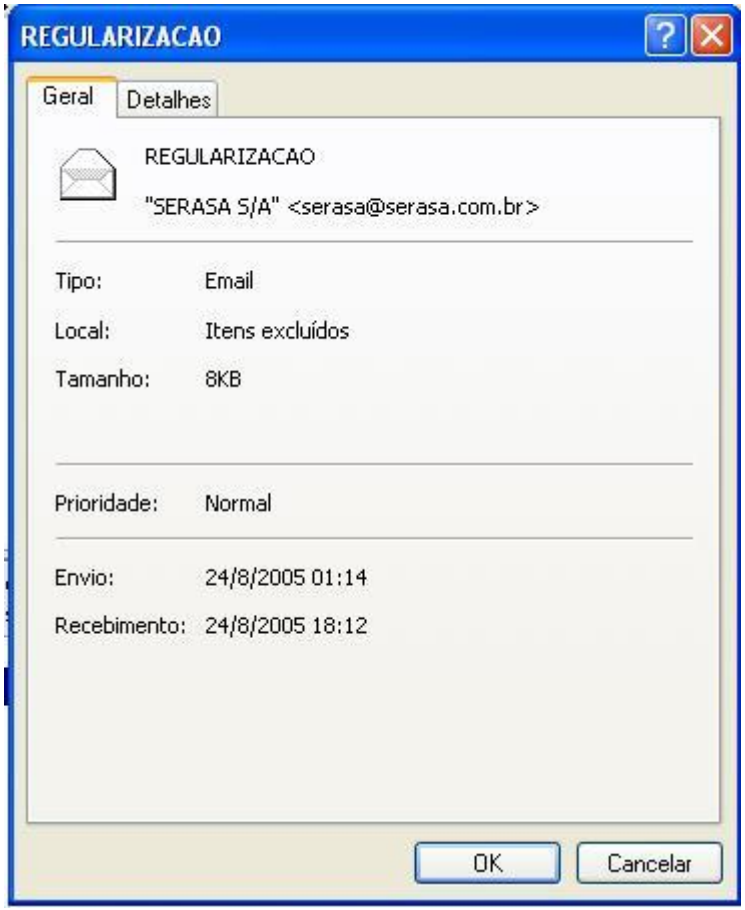


Principal

Phishing Scam



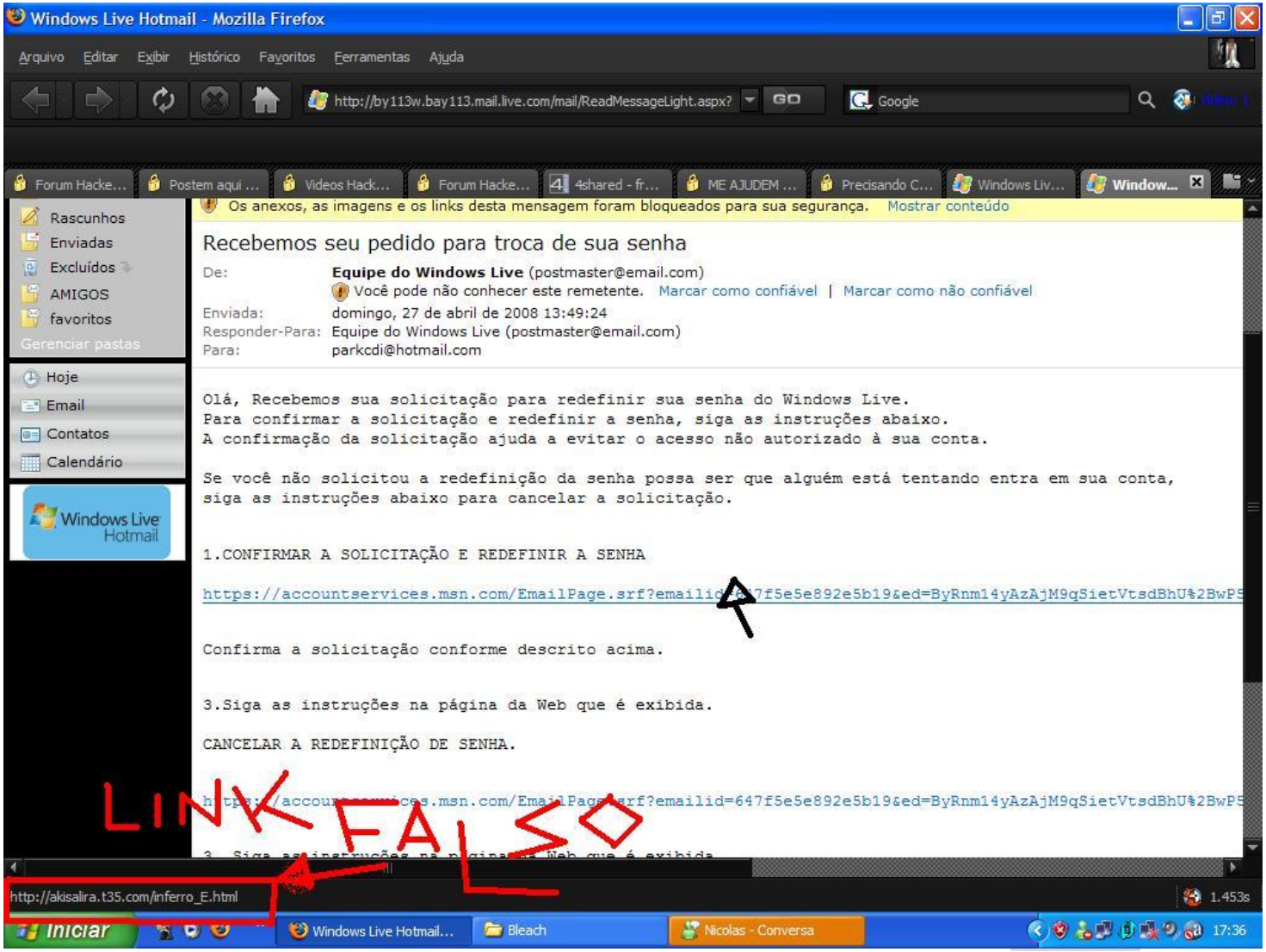
Phishing Scam



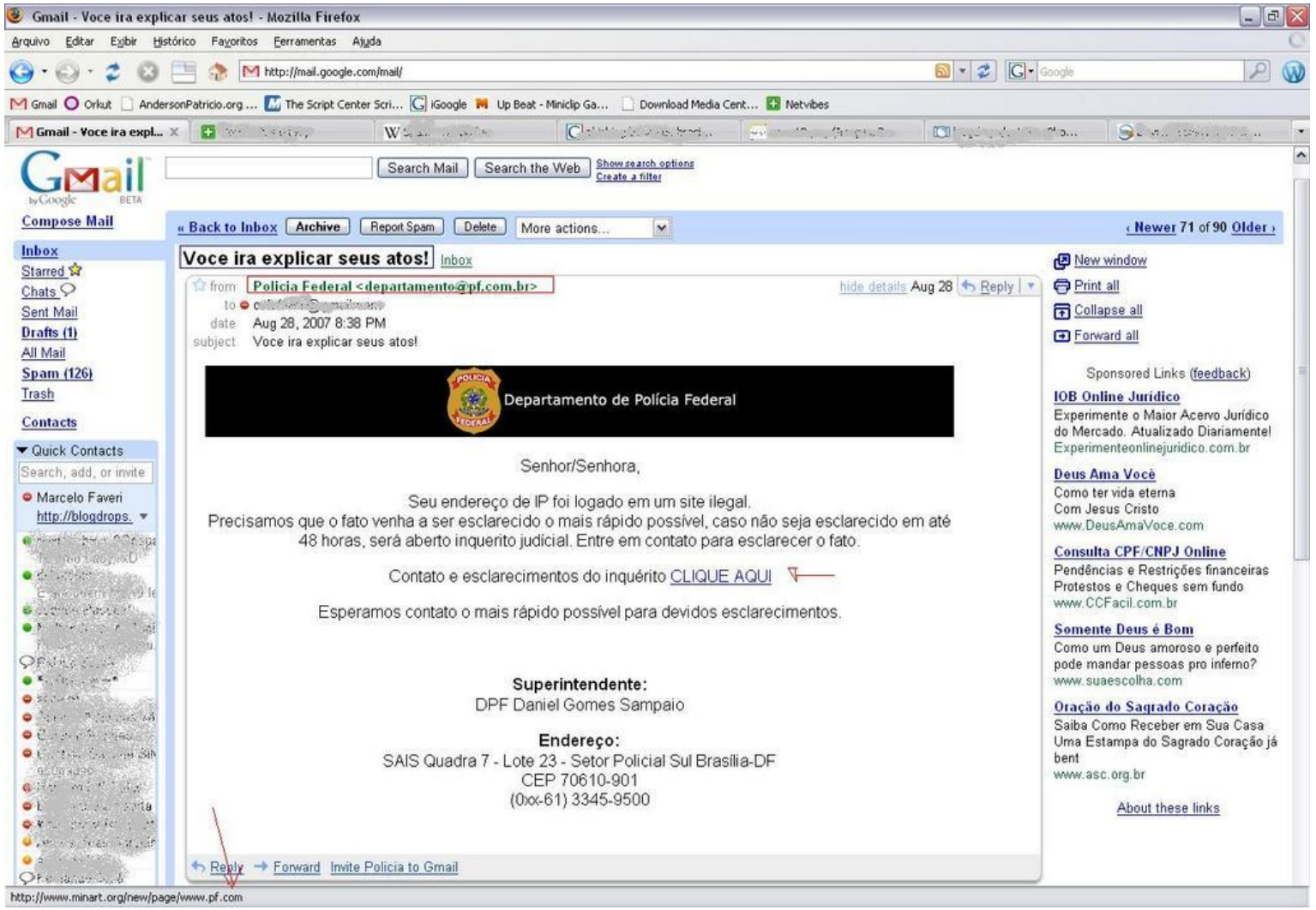
Phishing Scam

Principal

Phishing Scam

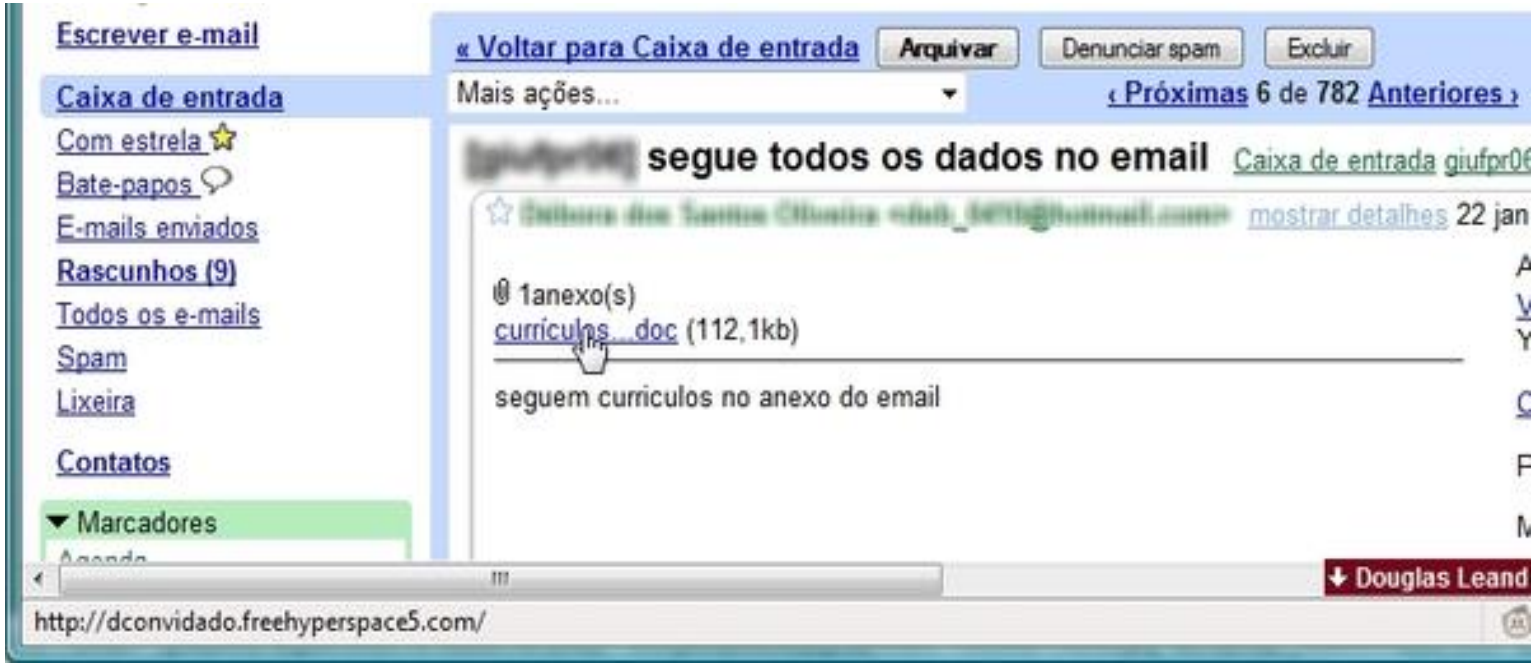


Phishing Scam

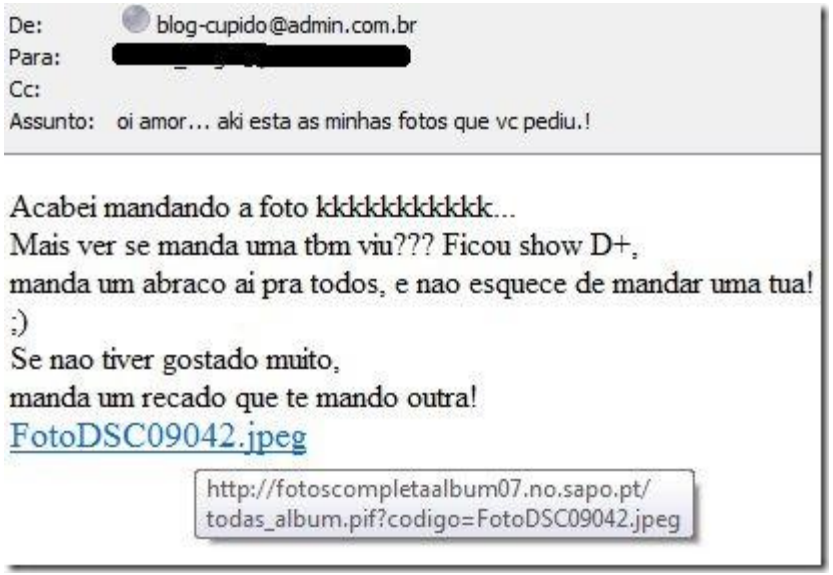


Principal

Phishing Scam



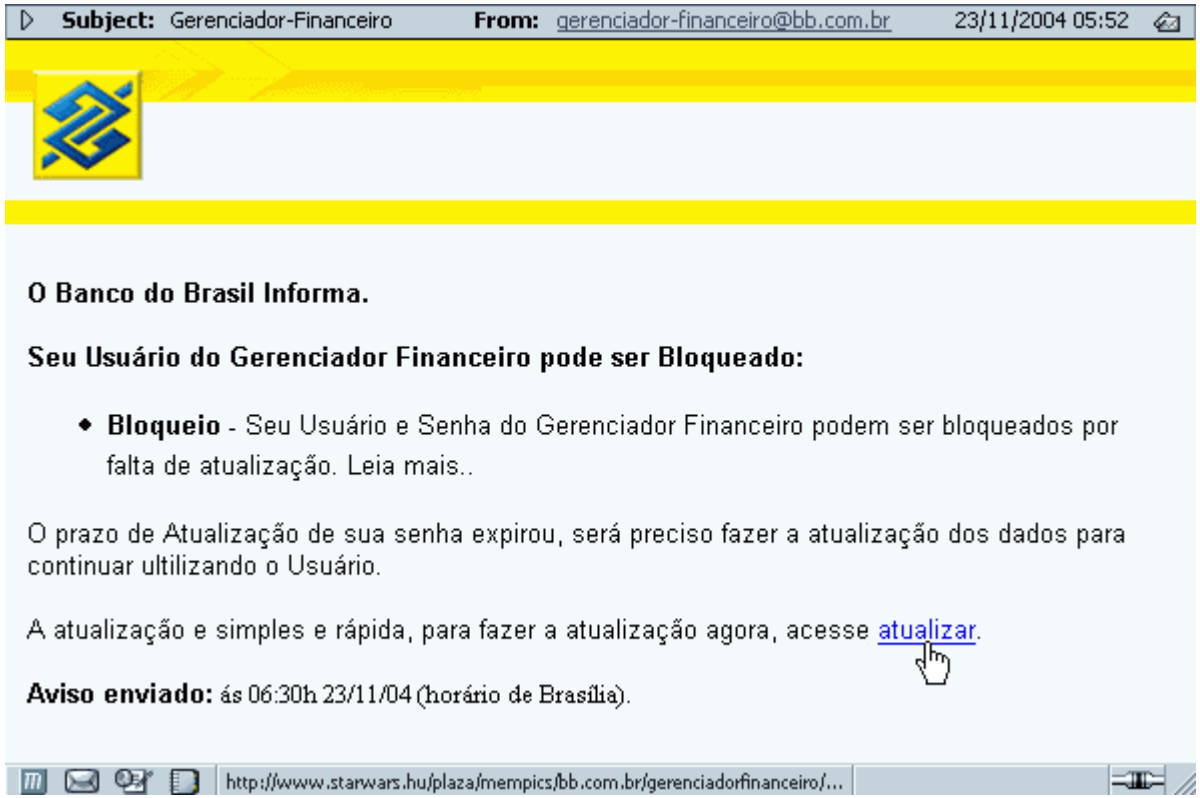
Phishing Scam


De: blog-cupido@admin.com.br
Para: [redacted]
Cc:
Assunto: oi amor... aki esta as minhas fotos que vc pediu.!

Acabei mandando a foto kkkkkkkkkkk...
Mais ver se manda uma tbm viu??? Ficou show D+,
manda um abraco ai pra todos, e nao esquece de mandar uma tua!
;)
Se nao tiver gostado muito,
manda um recado que te mando outra!
FotoDSC09042.jpeg

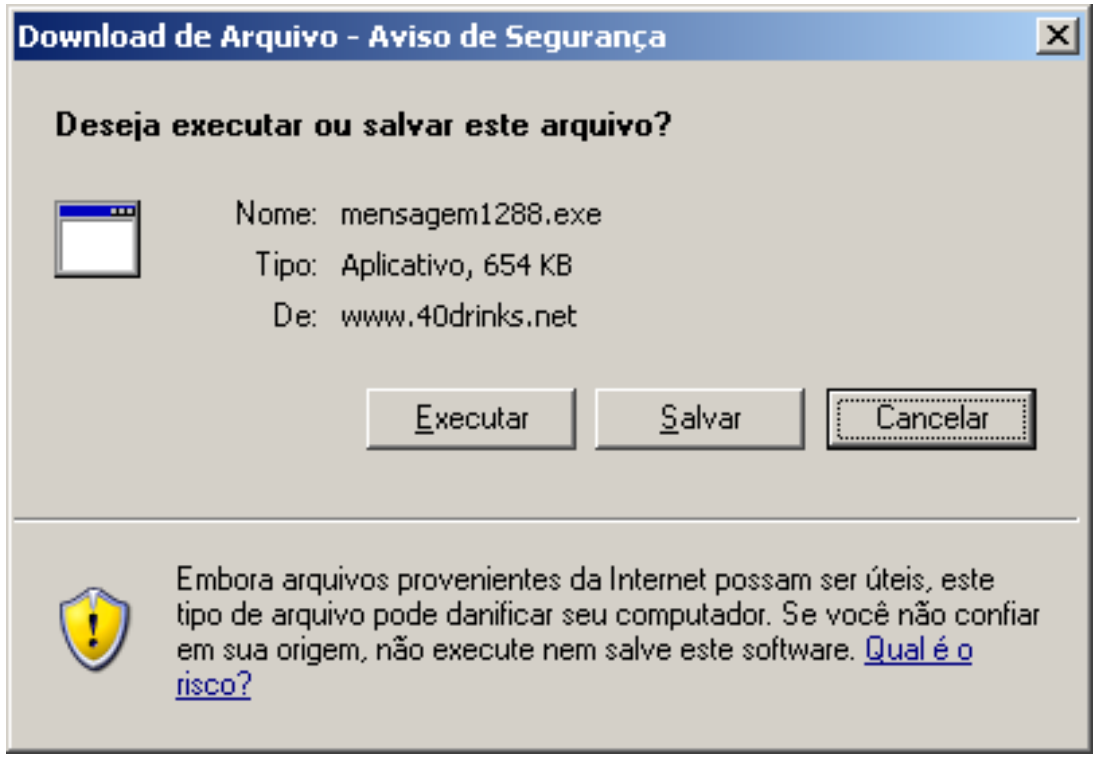
http://fotoscompletaalbum07.no.sapo.pt/
todas_album.pif?codigo=FotoDSC09042.jpeg

Phishing Scam



Principal

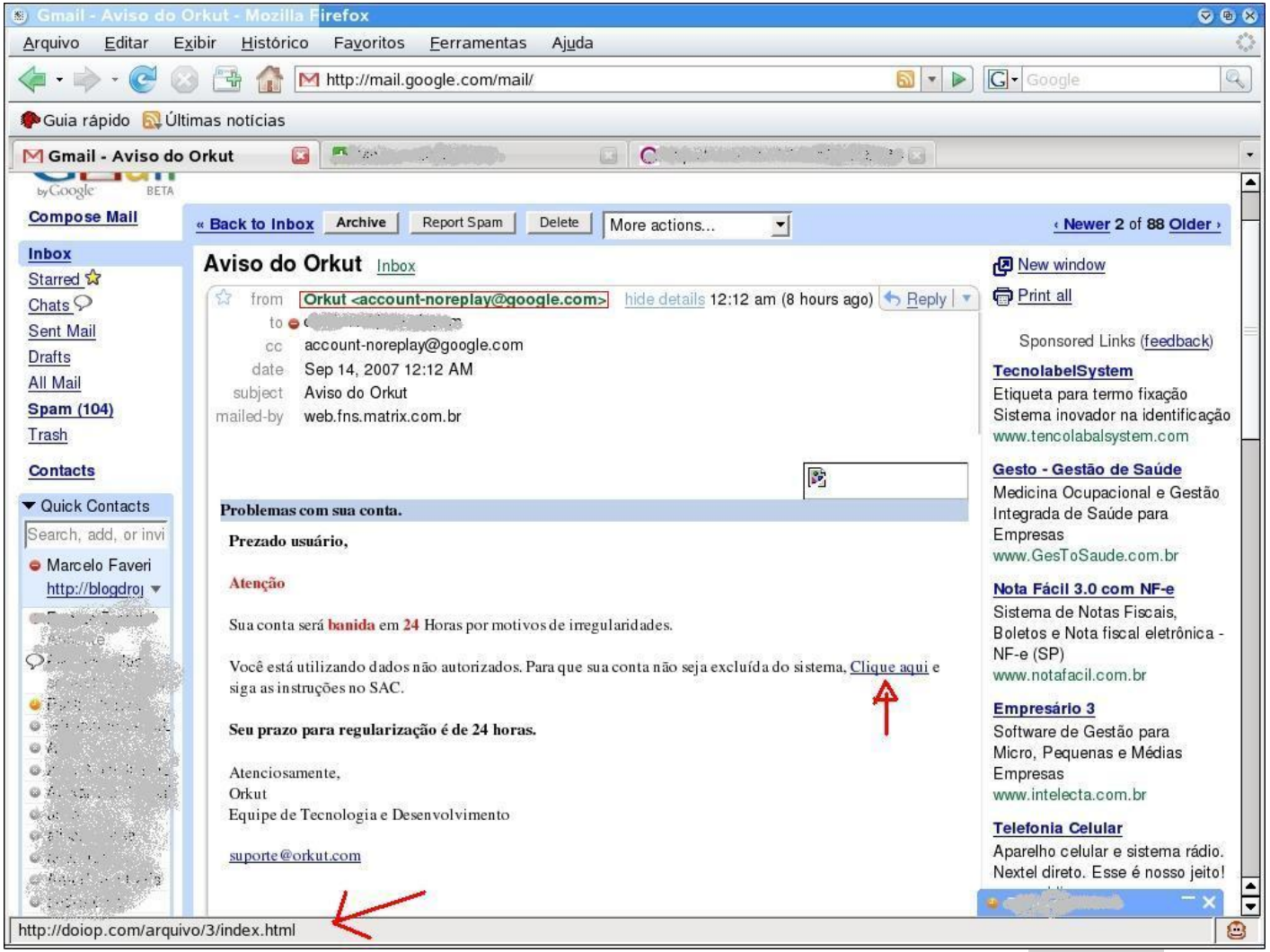
Phishing Scam



Phishing Scam

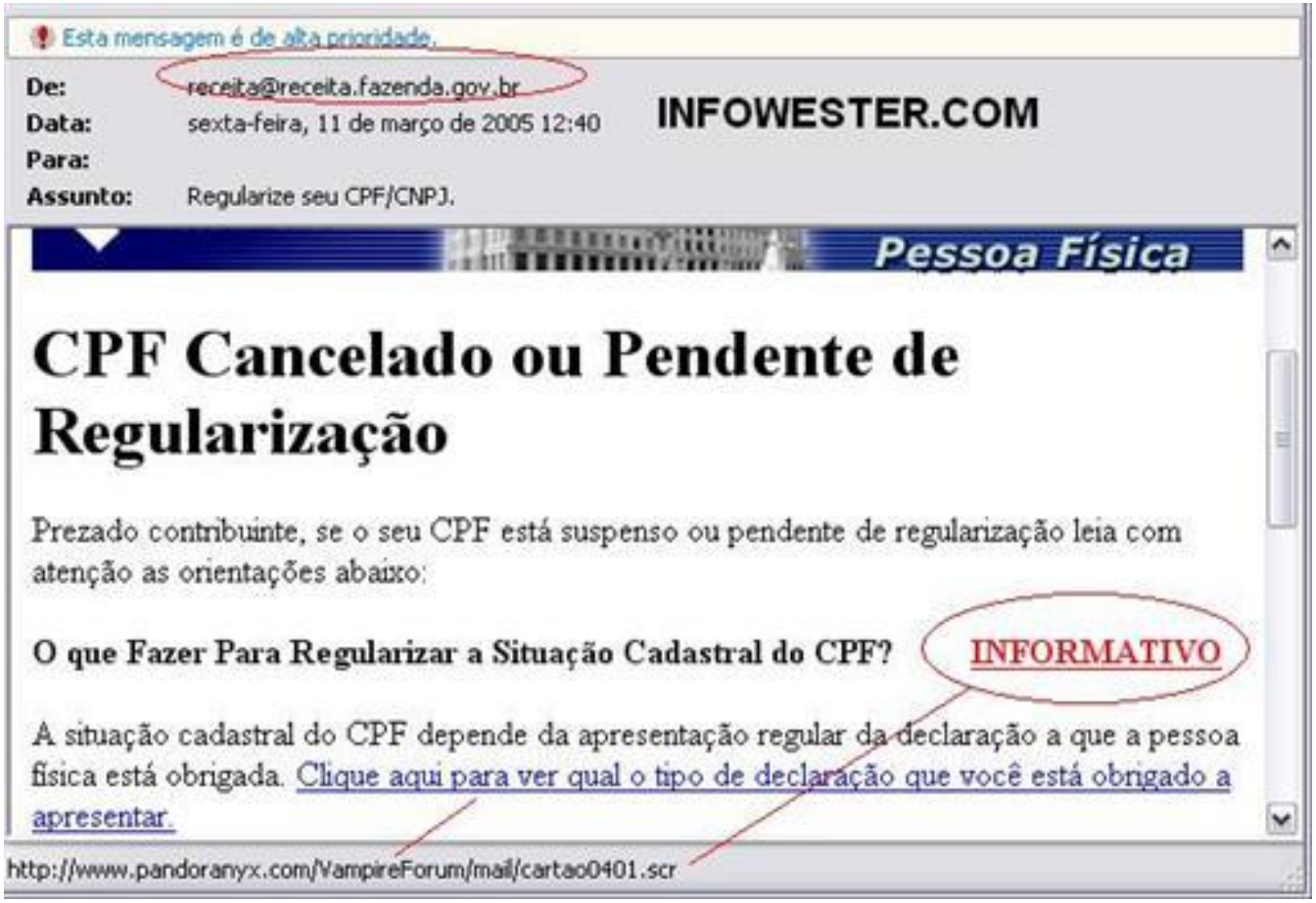
Principal

Phishing Scam

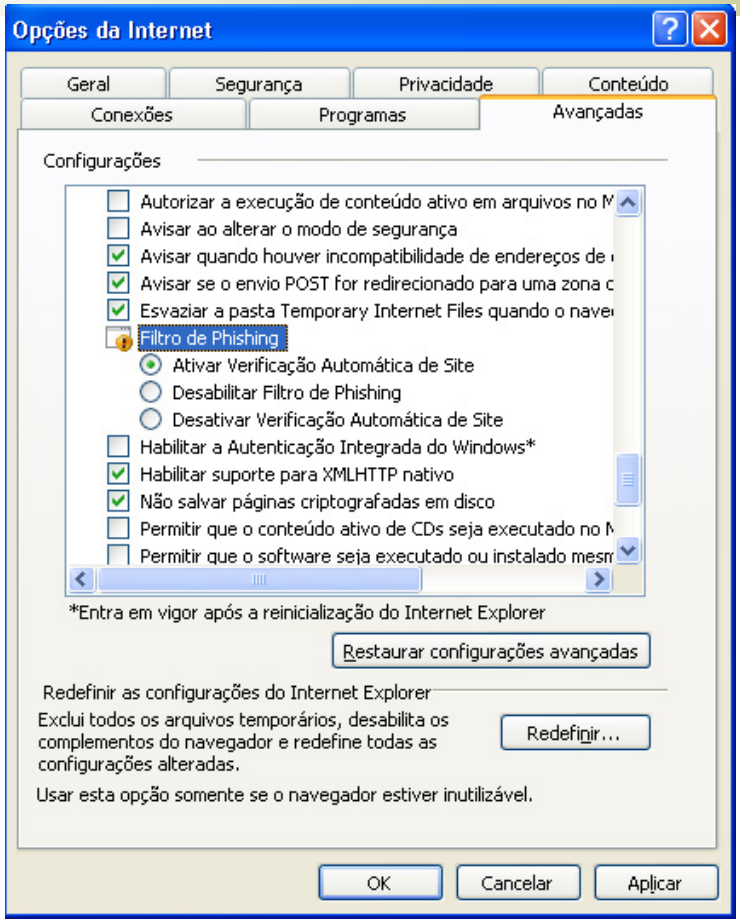


Principal

Phishing Scam



Phishing Scam



Identificação

- **Identificação de todos os ativos de informação importantes**

Ativo	Descrição
Hardware	Estações, computadores pessoais, impressoras, roteadores, *switches*, *modems*, servidores de terminal e *firewalls*
Software	Código fonte, programas executáveis,utilitários, programas de diagnóstico, sistemas operacionais e programas de comunicação
Dados	Dados armazenados *online* e dados arquivados, *backups*, *logs* de auditoria, bancos de dados e dado em trânsito em meios de comunicação
Pessoas	Usuários, Administradores e operadores
Documentação	Manuais de programas, *hardware* interno, sistemas e procedimentos locais de administração

Identificação

- **Nível de criticidade**
  - Nível de importância dentro da instituição

Ativo	Classificação	Valoração	Criticidade
Correio eletrônico interno	Administrativo	Moderado	Média
Salários dos empregados	Financeiro	Alto	Média
Tendências de mercado	Pesquisa	Baixo	Baixa
Patentes pendentes	Proprietário	Alto	Alta
Balanço anual	Financeiro	Moderado	Alta

Vulnerabilidades e ameaças

Vulnerabilidade

- Evidência ou fragilidade que eleva o grau de exposição do ativo, aumentando a probabilidade de sucesso da investida de uma ameaça
- É preciso conhecer as vulnerabilidades de cada ativo

Vulnerabilidades		
Físicas	Tecnológicas	Humanas
Cabeamento de baixa qualidade	Defeito de software	Falta de conscientização dos usuários
Ausência de fragmentadora de papel	Sistema operacional desatualizado	Ausência de rotinas de backup
Instalação elétrica mal dimensionada	Senha fraca	Descuido e despreparo

Calculando

- **Neste cenário temos 50 empregados ociosos:**
  - 8 (horas/dia) x 240 (dias/ano) x 50 (número de pessoas) = 96.000 horas
  - R$ 50,00 (custo/hora) x 96.000 (horas) = R$ 4.800.000,00
  - Custo direto (fixo) da empresa com os 50 funcionários durante um ano: R$ 4.800.000,00

Segurança da Informação

A segurança da informação transcende a informática

- Não existe sistema 100% seguro
- O elo mais fraco da corrente sempre será o ser humano
- Os riscos e as vulnerabilidades transcendem o mundo tecnológico
- Vulnerabilidades físicas, tecnológicas e humanas estarão sempre presentes

Questões

- Por que sistemas de informação são tão vulneráveis a destruição, erro, uso indevido e problemas de qualidade de sistemas?
- Que tipos de controles estão disponíveis para os sistemas de informação?
- Que medidas especiais devem ser tomadas para assegurar a confiabilidade, a disponibilidade e a segurança em processos de comércio eletrônico e negócios digitais?
- Quais são as técnicas mais importantes para garantir a qualidade de um software?
- Por que a auditoria dos sistemas de informação e a salvaguarda da qualidade dos dados são tão importantes?

SEGURANÇA EM TI

Tiago Alves de Oliveira

toliveira@divinopolisuemg.com.br