Eu estou seguro ?

Humberto Sartini
http://web.onda.com.br/humberto

Palestrante

Humberto Sartini

- Analista de Segurança do Provedor Onda S/A
- Participante dos projetos:
  - Rau-Tu Linux (http://www.rau-tu.unicamp.br/linux)
  - HoneypotBR (http://www.honeypot.com.br/)
- Participante do:
  - IV Fórum Internacional de SL (Porto Alegre – 2003)
  - Conferência Internacional de SL (Curitiba - 2003)
  - CBN Debate – Tema: Internet (Curitiba – 2004)
  - Sucesu-PR – Servidor Postfix (Curitiba – 2004)

Tópicos

- Situação Atual
- Legislação
- O que o usuário pode fazer ?
- O que o administrador pode fazer ?
- Casos e Exemplos

Situação Atual

DESORDEM

Situação Atual

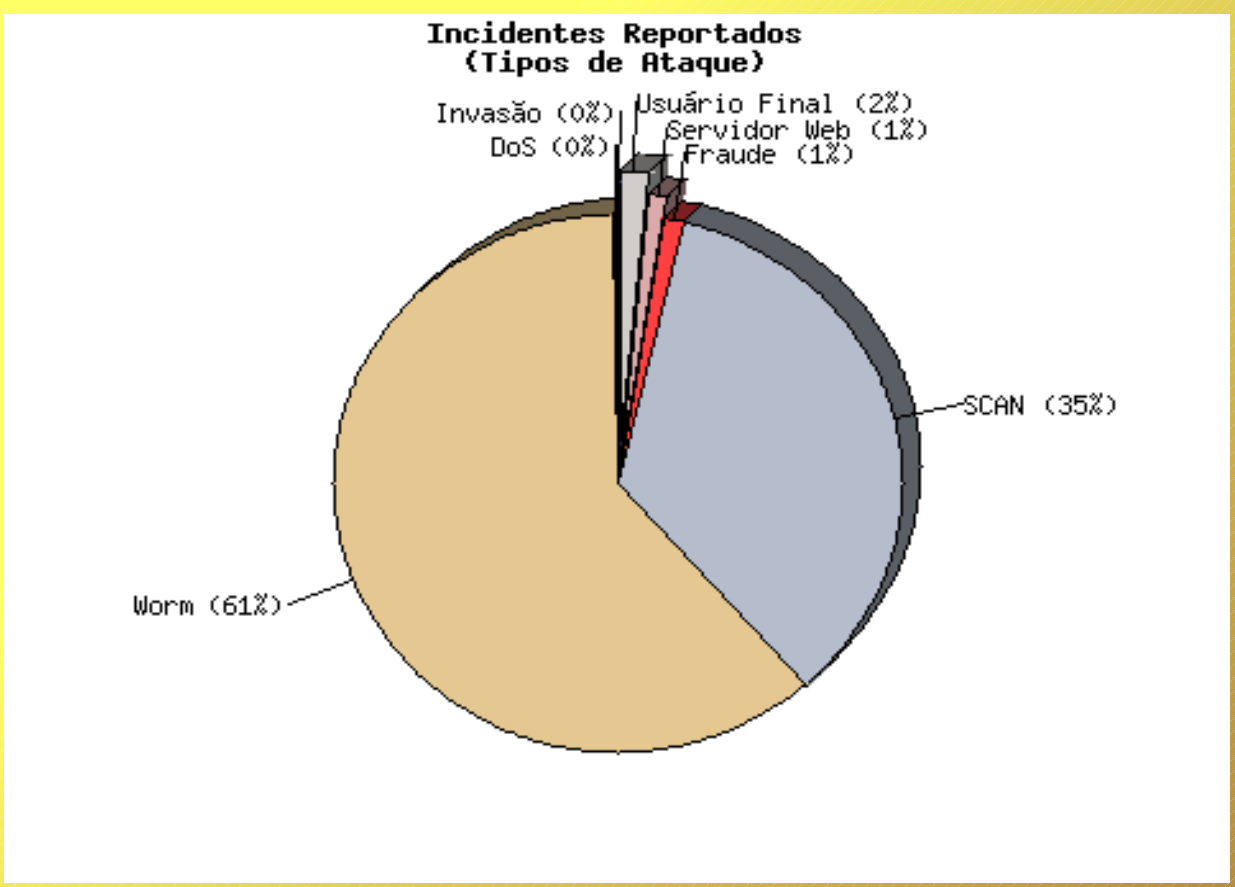
Podemos dividir a situação atual em:

- Incidentes:
  (D)Dos, Fraudes, Invasões, Scan, Worms, Trojans e Vírus

- Spam:
  Proxy Aberto, Relay Aberto e Spamvertised Website

Situação Atual - Incidentes

Incidentes Reportados ao NBSO
(Janeiro a Dezembro de 2003)



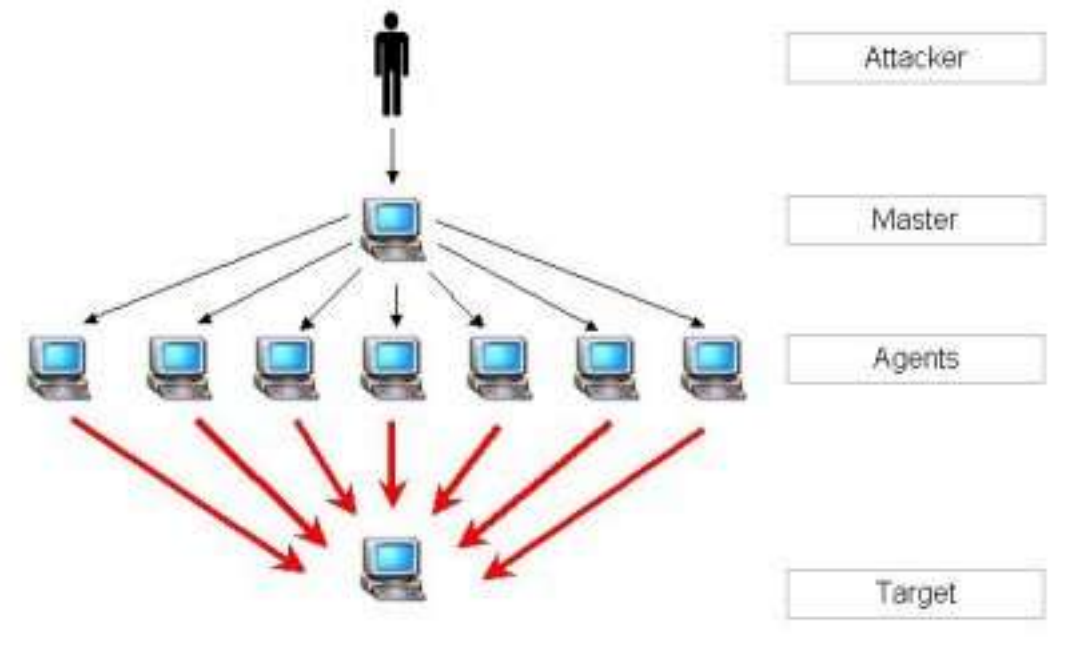
Situação Atual - Incidentes

(D)DOS: (Distributed) Denial Of Service

- Sobrecarga no processamento
- Grande Tráfego de Dados (Rede ou Host)
- Parada de Serviço (Temporário)
- Difícil detecção e solução

Situação Atual - Incidentes

- Funcionamento



Situação Atual - Incidentes

- Prevenção
  - Monitoração 24 horas
  - Equipe Especializada
  - Atuação durante o ataque

Situação Atual - Incidentes

FRAUDES

Engenharia Social

- Obtenção de dados pessoais através de ligações telefônicas ou e-mails
- Usar do Bom Senso

Situação Atual - Incidentes

FRAUDES

Internet Banking

- O cadeado não é sinal de total segurança
- Verificar a URL completa

Situação Atual - Incidentes

FRAUDES

Hoax (Boatos)

- Correntes e/ou pirâmides
- Pessoas doentes
- Nigéria (Transferência de Dólares)

http://www.iis.com.br/~cat/infoetc/562.htm

Situação Atual - Incidentes

INVASÕES

- Falhas de softwares (Versões obsoletas)
- Serviço com configuração incorreta

Situação Atual - Incidentes

INVASÕES

- Prevenção
  - Manter o sistema atualizado
  - Verificar configuração
  - Utilizar softwares de verificação de vulnerabilidades
  - Monitoramento

Situação Atual - Incidentes

SCAN

- Checagem de Vulnerabilidade de Serviços
- Detecção de Portas “Abertas”

Situação Atual - Incidentes

SCAN

- Prevenção
  - Utilização de ferramentas anti Scan (Scan Detect, Astaro Portscan Detection, Port Scan Attack Detector, etc ...)
  - Configuração correta Firewall

Situação Atual - Incidentes

WORMS (VERMES)

Situação Atual - Incidentes

WORMS

- Vírus inteligentes
- Capacidade de Multiplicação
- Entidades autônomas (Sem arquivo hospedeiro)
- Utilizam Internet para propagação

Situação Atual - Incidentes

WORMS

- Bagle (Variantes de “A”até “V”)
- Netsky (Variantes de “A”até “P”)
- Mydoom (Variantes de “A”até “H”)

- Permitem que a máquina seja utilizada como ponte em ataques DDOS

Situação Atual - Incidentes

WORMS

- Slammer
  - Falhas do Microsoft Sql Servers
  - Porta 1434/UDP
  - Lentidão Internet Mundial
  - Apagão dos EUA

Situação Atual - Incidentes

TROJAN (ou Cavalo de Tróia)

- Destruir o sistema
- Keyllogers
- Permite acesso remoto
- Não infecta outros arquivos

Situação Atual - Incidentes

TROJAN (ou Cavalo de Tróia)

- Code Red
  Falhas do IIS

- Nimda
  Checava mais de 100 falhas

Situação Atual - Incidentes

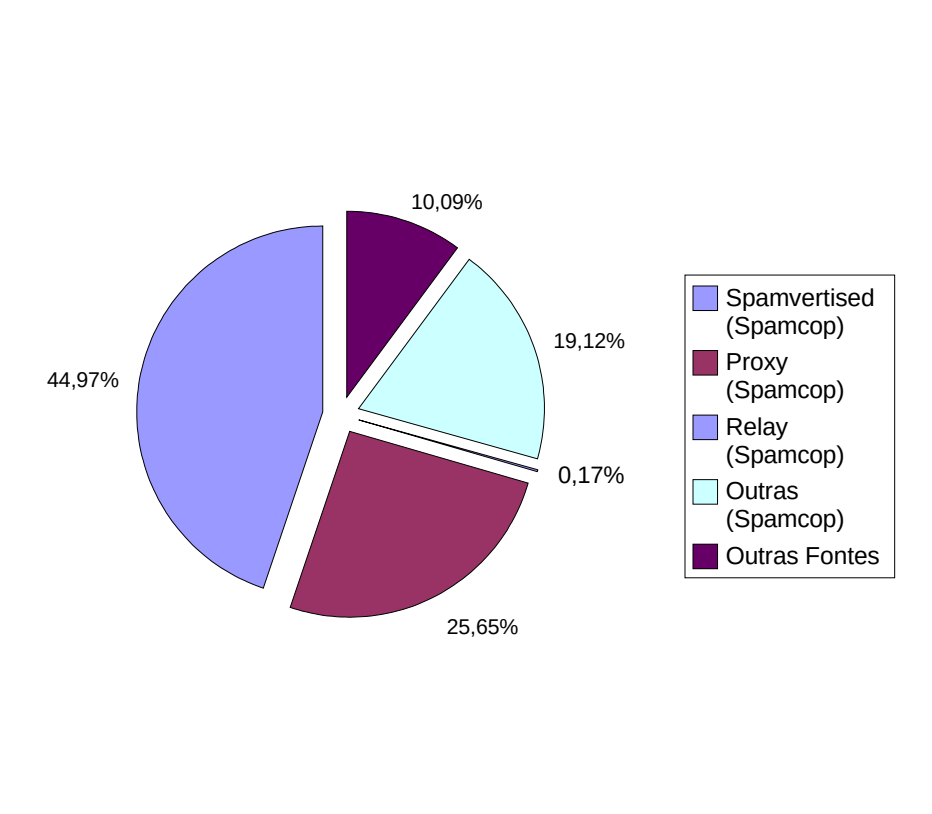
Worms, Trojan e Vírus

- Prevenção
  - Antivírus atualizado
  - Sistema atualizado
  - Verificar remetentes (pouco eficaz)
  - Deletar e-mail com anexo não solicitado (pouco eficaz)
  - Não instalar arquivos de P2P

Situação Atual - Spam

Situação Atual - Spam

Spams Reportados ao NBSO
(Janeiro a Dezembro de 2003)



Situação Atual - Spam

- Spam ou UCE (Unsolicited Commercial Email) nada mais é do que o envio de e-mails não solicitados

- Uma das principais perturbações para internautas, administradores de redes e provedores

- Problemas financeiros (saturação de links e pessoas para tratar do assunto)

Situação Atual - Spam

- Quais os objetivos do spam ?

1º Venda de Produtos
2º Venda de Produtos
3º Venda de Produtos
4º Instalação de Trojans

Situação Atual - Spam

- O primeiro SPAM foi um anúncio da DEC que falava sobre a nova máquina DEC-20, em 1978, na Arpanet.

- Um dos comentários mais curiosos é o do Richard Stallman, que não achava o spam um problema (na época), posição totalmente contrária à que tem hoje.

Situação Atual - Spam

- Proliferação do Spam no Brasil
  - Baixo custo de link Banda Larga
  - Listas de E-mails abundantes
  - Legislação Inexistente
  - Poucos problemas (infelizmente) para o spammer
  - Retorno “compensatório”

Situação Atual - Spam

- Exemplo de Retorno “compensatório”

20 milhões pessoas	100%
2 milhões pessoas	10%
200 mil pessoas	1%
20 mil pessoas	0,1%
2 mil pessoas	0,01%
200 pessoas	0,001%
20 pessoas	0,0001%
2 pessoas	0,00001%

Situação Atual - Spam

- Como são enviados os spam ?
  - Geralmente são utilizados links de Banda Larga (ADSL, Rádio, TV a Cabo)
  - Origem da própria máquina ou através de servidores com confi-gurações incorretas (Open Proxy e Open Relay)

Situação Atual - Spam

PROXY ABERTO

- Servidor de Proxy mal configurado, permitindo que a máquina seja utilizada para envio de spam

- Configurar corretamente o servidor de Proxy

Situação Atual - Spam

RELAY ABERTO

- Servidor de E-mail mal configurado, permitindo que a máquina seja utilizada para envio de spam

- Configurar corretamente o servidor de E-mail

Situação Atual - Spam

SPAMVERTISED WEBSITE

- Máquinas que hospedam páginas com produtos e serviços sendo oferecidos no spam

- AOL começou a bloquear o acesso desses sites pelos seus assinantes (29/03/2004)

Legislação

Legislação

- Não temos Legislação Federal
- Vários Projetos de Leis
- Definições diferentes de SPAM

Legislação

Projeto de Lei (PL) 84/99

- Primeira legislação específica brasileira sobre crimes de informática

- Aprovada no Plenário da Câmara Federal, em novembro de 2003

- Parecer favorável, do senador Marcelo Crivella (PL-RJ) ao Projeto de Lei (PL) 84/99, que tramita atualmente pelo Senado Federal como PLC 89/2003

Legislação

Projeto de Lei (PL) 84/99

- Ementa: Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências.

- Explicação da Ementa: Caracterizando como crime os ataques praticados por "hackers" e "crackers", em especial as alterações de "home pages" e a utilização indevida de senhas.

Legislação

Projeto de Lei (PL) 84/99

“Falsidade Informática”

Art. 154-C. Introduzir, modificar, apagar ou suprimir dado ou sistema informatizado, ou, de qualquer forma, interferir no tratamento informático de dados, com o fim de obter, para si ou para outrem, vantagem indevida de qualquer natureza, induzindo a erro os usuários ou destinatários. Pena - detenção, de um a dois anos, e multa.

Parágrafo único. Nas mesmas incorre quem, com a mesma finalidade, cria, disponibiliza ou divulga comunicação eletrônica falsa.

Legislação

Projeto de Lei (PL) 84/99

“Sabotagem Informática”

Art. 154-D. Introduzir, modificar, apagar ou suprimir dado ou sistema informatizado, ou, de qualquer forma, interferir em sistema informatizado, com o fim de desorientar, embaraçar, dificultar ou obstar o funcionamento de um sistema informatizado ou de comunicação de dados à distância.

Pena - detenção, de um a dois anos, e multa.

Legislação

Grupo Brasil Anti Spam – Abranet, Abap, Abes, entre outras
http://www.brasilantispam.org/

Artigo 3º. – “Spam” - é a designação para a atividade de envio de Mensagens Eletrônicas e Mala Direta Digital que não possam ser consideradas nem Marketing Eletrônico, nem Newsletter, e nas quais se verifique a simultânea ocorrência de pelo menos 2 (duas) das seguintes situações:

a) Inexistência de identificação ou falsa identificação do Remetente;

b) Ausência de prévia autorização (opt-in) do Destinatário;

c) Inexistência da opção “opt-out”;

Legislação

d) Abordagem enganosa – tema do assunto da mensagem é distinto de seu conteúdo de modo a induzir o destinatário em erro de acionamento na mensagem;

e) Ausência da sigla NS no campo Assunto, quando a mensagem não houver sido previamente solicitada;

f) Impossibilidade de identificação de quem é de fato o Remetente;

g) Alteração do Remetente ou do Assunto em mensagens de conteúdo semelhante e enviadas ao mesmo Destinatário com intervalos inferiores a 10 (dez) dias.

Legislação

Extorsão por e-mail deve ser julgada no PR

No caso de mensagens eletrônicas ameaçadoras, enviadas pela rede mundial de computadores (internet), o crime se consuma onde as vítimas as receberam, e não no local de onda foram enviadas. O entendimento é da Terceira Seção do Superior Tribunal de Justiça (STJ).

Fonte: Jornal O Estado do Paraná – 23/03/2004

Legislação

"... pouco importa o local de onde foram enviadas as últimas mensagens eletrônicas, pois o crime de extorsão se cosumou no lugar no qual os ofendidos receberam os e-mails e deles tomaram conhecimento, no caso, na cidade em que se situa a sede da empresa administrada pelas pessoas extorquidas."

Fonte: Jornal O Estado do Paraná – 23/03/2004

Legislação

- Ministério da Defesa

PORTARIA NORMATIVA Nº 333/MD, DE 24 DE MARÇO DE 2004

Dispõe sobre a Política de Guerra Eletrônica de Defesa.

Legislação

Art. 4º A definição dos objetivos e a determinação das diretrizes da Política de Guerra Eletrônica obedecem aos seguintes pressupostos básicos:

I - as atividades de Guerra Eletrônica nas Forças Armadas são orientadas para atender às necessidades da defesa nacional;

II - a capacitação tecnológica é buscada de maneira harmônica com a Política de Defesa para a área de Ciência e Tecnologia;

III - as atividades de Guerra Eletrônica nas Forças Armadas são conduzidas de modo a assegurar o uso do espectro eletro-magnético por nossas forças e impedir, reduzir ou prevenir seu uso contra os interesses do país; e

IV - a eficácia das ações direcionadas à implementação da Guerra Eletrônica nas Forças Armadas depende diretamente do grau de conscientização alcançado junto às organizações e pessoas acerca do valor da informação que detêm ou processam.

Legislação

Art. 5º São objetivos da Política de Guerra Eletrônica de Defesa:
I - interoperabilidade das atividades de Guerra Eletrônica desenvolvidas pelas Forças Armadas;
II - ordenamento do intercâmbio entre as instituições de pesquisa das Forças Armadas no que se refere às atividades relacionadas com a Guerra Eletrônica;
III - capacitação dos recursos humanos necessários à condução das atividades de Guerra Eletrônica;
IV - capacitação das Forças Armadas para a utilização simultânea do espectro eletromagnético, com segurança e sem interferência mútua;
V - implementação da mentalidade de Guerra Eletrônica desde o início da formação militar, em todos os níveis, nas Forças Armadas;
VI - acompanhamento da evolução doutrinária e tecnológica da Guerra Eletrônica nos âmbitos nacional e internacional;
VII - ordenamento do intercâmbio entre as instituições de ensino de Guerra Eletrônica das Forças Armadas; e
VIII - redução do grau de dependência externa em relação a sistemas, equipamentos, dispositivos e serviços vinculados à Guerra Eletrônica, de interesse dos componentes da expressão militar do Poder Nacional.

O que o usuário pode fazer ?

- Lado mais fraco

Para variar o usuário é o lado mais fraco, uma vez que é dependente de serviços de Telecom e não tem muita voz ativa.

Algumas ações podem ser efetuadas pelo usuário, que são:

O que o usuário pode fazer ?

- Antivírus Atualizado
- Manter o sistema e os programas atualizados
- Não ficar enviando correntes e pirâmides
- Não cadastrar seus dados em qualquer site e ler as Políticas de Privacidade

O que o usuário pode fazer ?

- Fazer comércio eletrônico em lojas conhecidas

- Em caso de SPAM ou tentativa de invasão entrar em contato com o departamento de ABUSE do fornecedor do acesso a Internet

- Ler as cartilhas do NIC BR, no site http://www.nbso.nic.br/docs/cartilha/

O que o usuário pode fazer ?

- Utilização de certificados digitais

  Desvantagem: Complexo para o usuário doméstico

  Vantagem: Prova que “você é você”

  Onde obter gratuitamente:
  http://www.thawte.com/email/index.html

O que o administrador pode fazer ?

O Administrador tem maiores poderes em auxiliar na diminuição de incidentes e spam.

Utilizando alguns métodos e práticas altamente difundidos, é possível diminuir os problemas que foram discutidos.

Entre eles podemos citar:

O que o administrador pode fazer ?

- Implantação de Política de Segurança

Não importa o tamanho ou segmento da empresa, é de suma importância elaborar uma Política de Segurança, para garantir que não venha a ocorrer problemas futuros.

Um exemplo de Política de Segurança pode ser encontrado em:

http://web.onda.com.br/humberto/psi.html

O que o administrador pode fazer ?

- Implantação do Departamento de Abuse

Quando a organização detêm a delegação do IP, é altamente recomendado ter um Departamento de Abuse, para tratar de incidentes e spam.

Um exemplo de implantação do Departamento de Abuse pode ser encontrado em:

http://www.nic.br

O que o administrador pode fazer ?

- Utilizar ferramentas “hacker”

Para saber o que pode ocorrer em sua rede, a melhor solução é tentar invadir !!

Existem “milhões” de programas que irão auxiliar nessa tarefa

Casos e Exemplos

- Clone do Internet Banking Itau
- Clone do Internet Banking Banco do Brasil

Banco Itaú - Feito Para Você - Microsoft Internet Explorer

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

Endereço http://211.56.233.205:9870 Ir Links

Itaú itaú Bankline AGÊNCIA CONTA OK >> Itaú em um clique

Abra sua Conta | Para Você | Personnalité | Private Bank | Empresas | Corporate Bank | Poder Público

Conheça o Itaú | Conta Corrente | Investimentos | Vida e Previdência | Cartões de Crédito | Empréstimos | Seguros | Acesso Internet

Faça um plano de previdência Itaú. E invista na sua vida.

Saiba mais Contrate já

DICA DO BANKLINE

Veja as informações sobre **Planos de Previdência** no Itaú Bankline

CLIQUE AQUI

SUPERNOVAS

Itaú Cultural

Acompanhe debate on-line sobre Educação e Cidadania. Dia 2/7, às 10h.

Prêmio Itaú-Unicef 5ª edição

As incrições foram prorrogadas. Não Perca!

Itauresidência Premiável

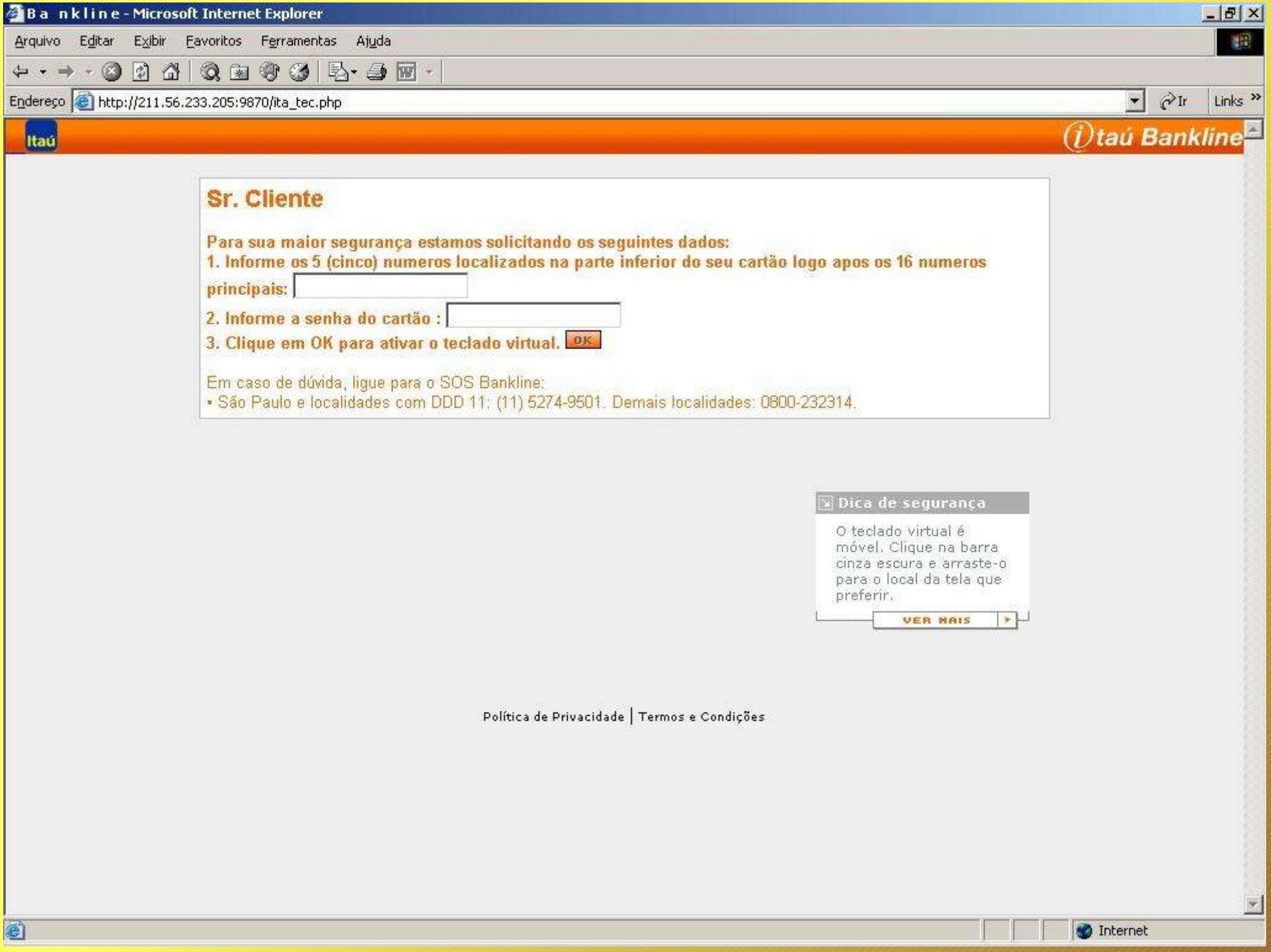
Proteja sua casa e concorra a R$25 mil por mês.

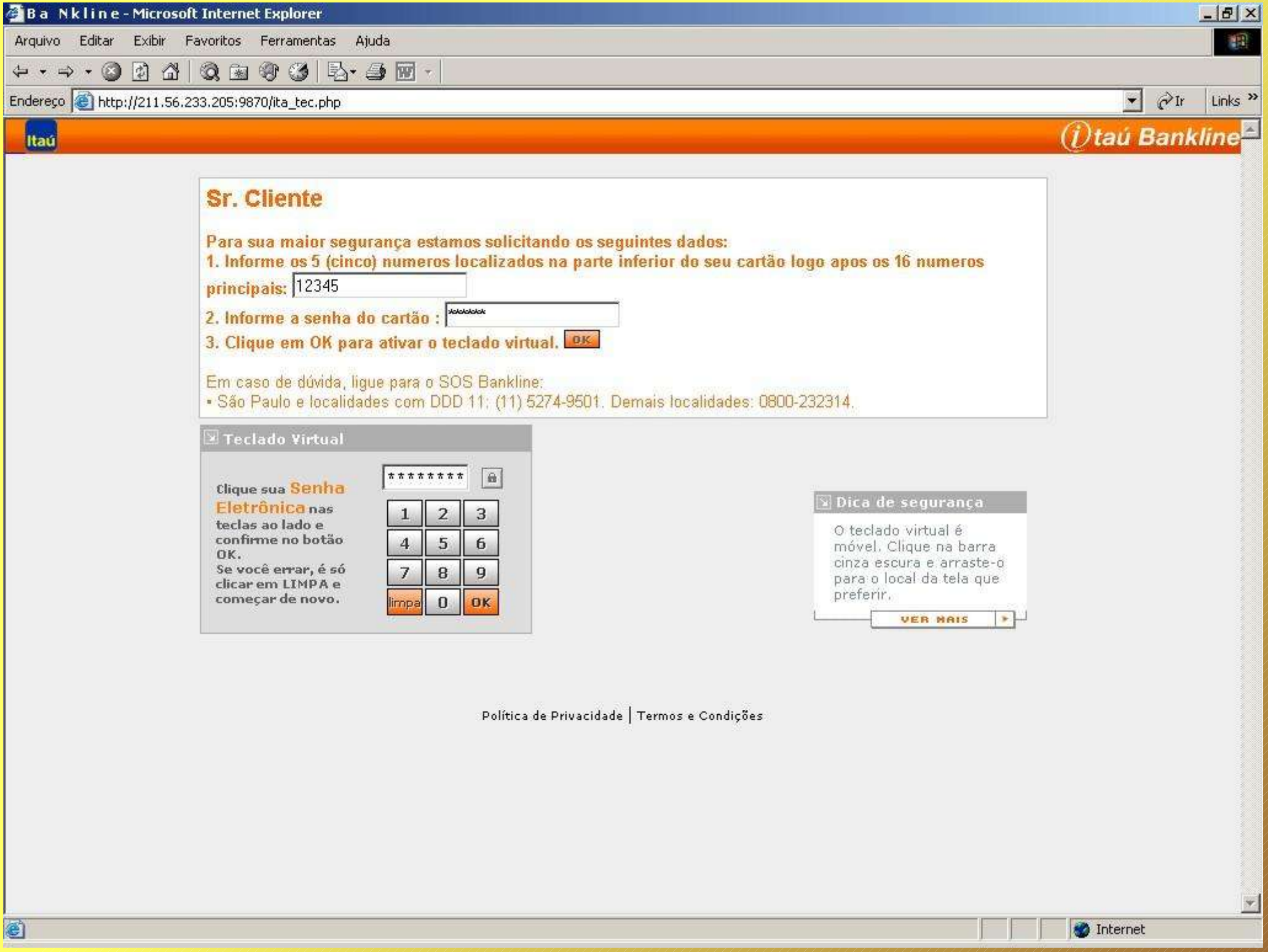
Itauvest Plus

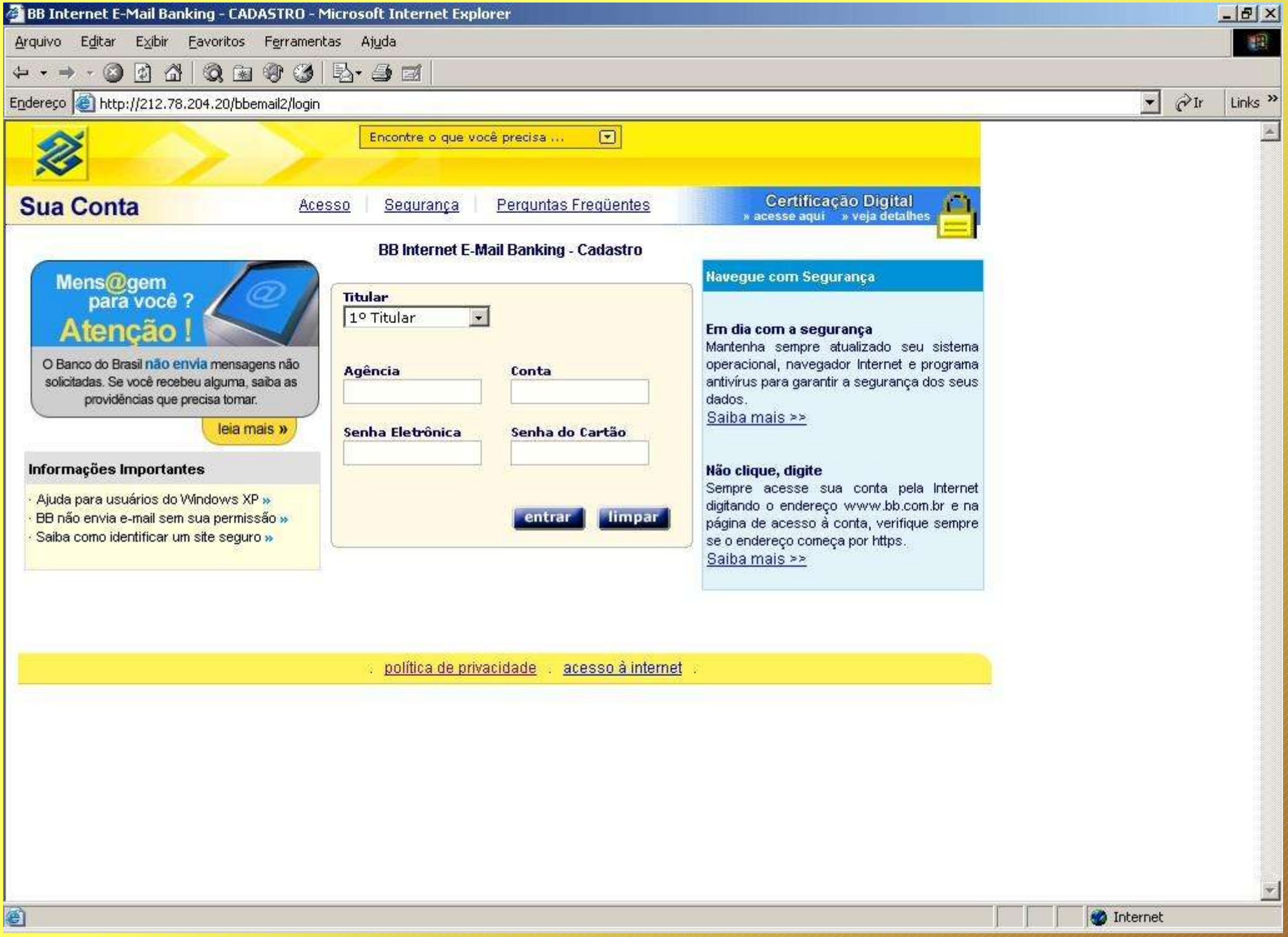
Comodidade para investir e sorte para concorrer a 5 Ford Fiesta por mês.

Relações com Investidores | Notícias e Cotações | Itaú Cultural | Itaú Social | Oportunidades de Carreira | Segurança e Privacidade | Fale Conosco

Internet


Ba nkline - Microsoft Internet Explorer
Arquivo Editar Exibir Favoritos Ferramentas Ajuda
Endereço http://211.56.233.205:9870/ita_tec.php
Ir
Links
Itaú
itaú Bankline
Sr. Cliente
Para sua maior segurança estamos solicitando os seguintes dados:
1. Informe os 5 (cinco) numeros localizados na parte inferior do seu cartão logo apos os 16 numeros principais:
2. Informe a senha do cartão :
3. Clique em OK para ativar o teclado virtual.
OK
Em caso de dúvida, ligue para o SOS Bankline:
• São Paulo e localidades com DDD 11: (11) 5274-9501. Demais localidades: 0800-232314.
Dica de segurança
O teclado virtual é móvel. Clique na barra cinza escura e arraste-o para o local da tela que preferir.
VER MAIS
Política de Privacidade | Termos e Condições
Internet


Ba Nkline - Microsoft Internet Explorer
Arquivo Editar Exibir Favoritos Ferramentas Ajuda
Endereço http://211.56.233.205:9870/ita_tec.php
Ir
Links
Itaú
itaú Bankline
Sr. Cliente
Para sua maior segurança estamos solicitando os seguintes dados:
1. Informe os 5 (cinco) numeros localizados na parte inferior do seu cartão logo apos os 16 numeros principais: 12345
2. Informe a senha do cartão :
3. Clique em OK para ativar o teclado virtual. OK
Em caso de dúvida, ligue para o SOS Bankline:
• São Paulo e localidades com DDD 11: (11) 5274-9501. Demais localidades: 0800-232314.
Teclado Virtual
Clique sua Senha Eletrônica nas teclas ao lado e confirme no botão OK.
Se você errar, é só clicar em LIMPA e começar de novo.
****
1 2 3
4 5 6
7 8 9
limpa 0 OK
Dica de segurança
O teclado virtual é móvel. Clique na barra cinza escura e arraste-o para o local da tela que preferir.
VER MAIS
Política de Privacidade | Termos e Condições
Internet


BB Internet E-Mail Banking - CADASTRO - Microsoft Internet Explorer
Arquivo Editar Exibir Favoritos Ferramentas Ajuda
Endereço http://212.78.204.20/bbemail2/login
Ir
Links
Encontre o que você precisa ...
Sua Conta
Acesso
Segurança
Perguntas Freqüentes
Certificação Digital
» acesse aqui
» veja detalhes
BB Internet E-Mail Banking - Cadastro
Mens@gem para você ?
Atenção !
O Banco do Brasil não envia mensagens não solicitadas. Se você recebeu alguma, saiba as providências que precisa tomar.
leia mais »
Informações Importantes
· Ajuda para usuários do Windows XP »
· BB não envia e-mail sem sua permissão »
· Saiba como identificar um site seguro »
Titular
1º Titular
Agência
Conta
Senha Eletrônica
Senha do Cartão
entrar
limpar
Navegue com Segurança
Em dia com a segurança
Mantenha sempre atualizado seu sistema operacional, navegador Internet e programa antivírus para garantir a segurança dos seus dados.
Saiba mais >>
Não clique, digite
Sempre acesse sua conta pela Internet digitando o endereço www.bb.com.br e na página de acesso à conta, verifique sempre se o endereço começa por https.
Saiba mais >>
política de privacidade
acesso à internet
Internet

AAPF - Microsoft Internet Explorer

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

Endereço http://65.77.42.232:7540/ Ir Links

Encontre o que você precisa ... BB Responde . Rede de Atendimento

Sua Conta

Acesso | Segurança | Perguntas Freqüentes

Certificação Digital
» acesse aqui » veja detalhes

Quem usa Internet Explorer 4.x precisa atualizar o **certificado do navegador** para acessar sua conta pela Internet. A instalação dura menos que **1 segundo**.

Instalar agora »
O que é isso ? »

Titular
1º Titular

Agência **Conta**

Senha de Auto-Atendimento

Problemas com o campo senha, **clique aqui**

entrar limpar

Informe o prefixo da agência.

Garanta a sua segurança »

O Banco do Brasil não envia e-mails sem a sua permissão!

Conheça as Mudanças

Simplificando o uso - A partir de agora você utilizará senhas apenas para entrar na sua conta e para transações com movimentação financeira.
Conheça os detalhes »

Novo teclado virtual - O novo teclado virtual é muito mais amigável. As principais novidades são: botões numéricos maiores, seqüência alterada, controle de luminosidade e posição centralizada na página.
Saiba mais »

Informações Importantes

- Ajuda para usuários do Windows XP »
- BB não envia e-mail sem sua permissão »
- Saiba como identificar um site seguro »

0800-785678 . política de privacidade . internet grátis . mapa do site

Internet

Contato

- Através do site ou e-mail

http://web.onda.com.br/humberto

humberto@onda.com.br

Links

- Google
http://www.google.com.br

- Jornal O Estado do Paraná
http://www.parana-online.com.br

- NIC Br
http://www.nbso.nic.br

- Módulo
http://www.modulo.com.br

- Scam Nigéria
http://www.iis.com.br/~cat/infoetc/562.htm

Links

- Senado Federal
http://www.senado.gov.br

- Sophos
http://www.sophos.com

- Thawte
http://www.thawte.com

Créditos

- Figura Slide 1:
http://www.artra.com.br/seguranca.jpg

- Figura Slide 4:
http://www.games-workshop.es/warhammer40k/campanas/ojo/images/ejercitos/caos-condenados.jpg

- Figura Slide 6:
http://www.nbso.nic.br/stats/incidentes/2003-jan-dec/tipos-ataque.png

- Figura Slide 8:
http://ingi2591.udev.org/pres/images/ddos.jpg

- Figura Slide 17:
http://koreabridge.com/photos/2003contest3/worms.jpg

- Figura Slide 24:
http://holyjoe.org/wallpaper/canospam.jpg

Créditos

- Figura Slide 25 (Criada através de dados obtidos em):
http://www.nbso.nic.br/stats/spam/2003-jan-dec/total.html

- Figura Slide 35:
http://www.idc.org.br/justica.gif

- Figuras Slide 52 a 56:
https://listas.unesp.br/mailman/listinfo/gts-l