Phishing e Malware:
as ameaças que chegam por SEDEX

Rogerio Bastos

https://certbahia.pop-ba.rnp.br

Quem somos

É responsável pela conexão das instituições baianas à rede acadêmica Brasileira (Rede Ipê) e operação da Rede Metropolitana de Salvador (Remessa).

É um CSIRT de coordenação para as instituições clientes do PoP-BA/RNP e parceiras da Remessa.

É mantido pelo PoP-BA/RNP em parceria com a UFBA.

Correio Eletrônico

Correio Eletrônico

- Utilização cresceu rapidamente

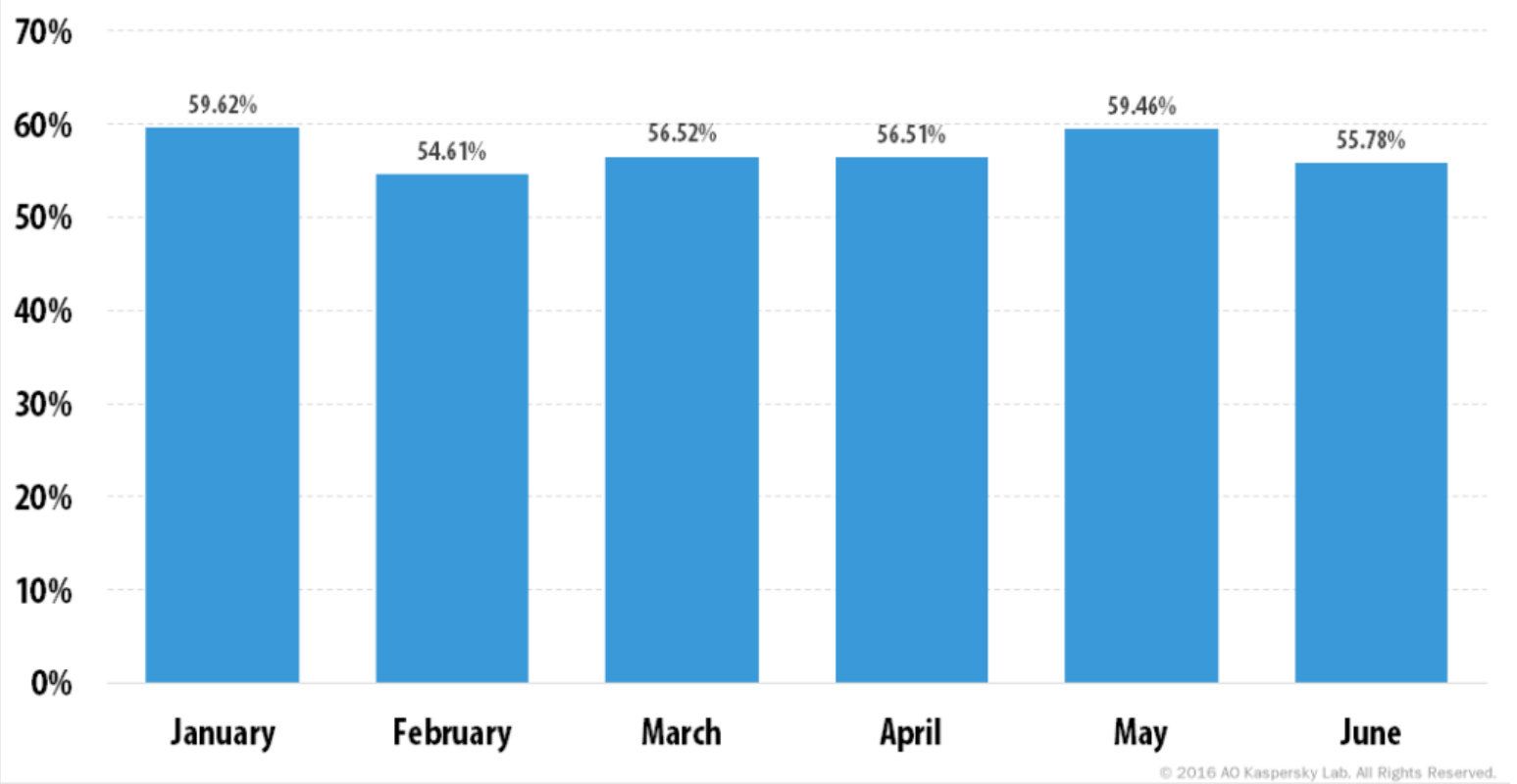
- Ferramenta de comunicação formal

	2015	2016
Worldwide Email Accounts (M)	**4,353**	**4,626**
%Growth		*6%*
Worldwide Email Users* (M)	**2,586**	**2,672**
% Growth		*3%*
Average Accounts Per User	1.7	1.7

Fonte: The Radicati Group – Email Statistics Report, 2015-2019

Correio Eletrônico

- Meio para práticas ilícitas



Fonte: SecureList Kaspersky – Spam and phishing in Q2 2016

Spam / Phishing / Scam

- **Spam**: envio em massa de mensagens não solicitadas.
- **Phishing**: tentativa de obter algum ganho se passando por uma entidade confiável.
- **Scam**: tentativa de obter a confiança através de engenharia social.

O Brasil é um grande alvo

Top 10 countries by percentage of attacked users

Japan	21.68%
Brazil	21.63%
India	21.02%
Ecuador	20.03%
Mozambique	18.30%
Russia	17.88%
Australia	17.68%
Vietnam	17.37%
Canada	17.34%
France	17.11%

Fonte: SecureList Kaspersky – Spam and phishing in 2015

O Brasil é um grande alvo

Top 10 countries by percentage of users attacked:

Brazil	21.5%
China	16.7%
United Kingdom	14.6%
Japan	13.8%
India	13.1%
Australia	12.9%
Bangladesh	12.4%
Canada	12.4%
Ecuador	12.2%
Ireland	12.0%

Fonte: SecureList Kaspersky – Spam and phishing in Q1 2016

O Brasil é um grande alvo

TOP 10 countries by percentage of users attacked:

China	20.22%
Brazil	18.63%
Algeria	14.3%
United Kingdom	12.95%
Australia	12.77%
Vietnam	11.46%
Ecuador	11.14%
Chile	11.08%
Qatar	10.97%
Maldives	10.94%

Fonte: SecureList Kaspersky – Spam and phishing in Q2 2016

Por que recebemos tanto spam?

- Fácil e barato enviar
- Difícil de rastrear
- Pode ser MUITO lucrativo
  - 90% dos spams são fraudes

Como funciona um phishing?

- Psicologia
  - Entidade confiável
  - Mais emoção => Menos razão
- Tecnologia
  - Maioria dos usuário não tem conhecimento básico
  - HTML, SMTP, DNS, HTTP, encoding

Manipulação Psicológica

Entidade Confiável

Procedimento Investigatório N.º 35482. 31/08/2016 (21589)

From: phishing@cais.rnp.br

To: phishing@cais.rnp.br

Ministério Público Federal

PROCEDIMENTO INVESTIGATÓRIO N.º 591812 OP. 01/08/2016

INTIMAÇÃO PARA COMPARECIMENTO EM AUDIÊNCIA, relativa ao procedimento investigatório em epígrafe, em tramitação nesta Regional, conforme despacho em anexo.

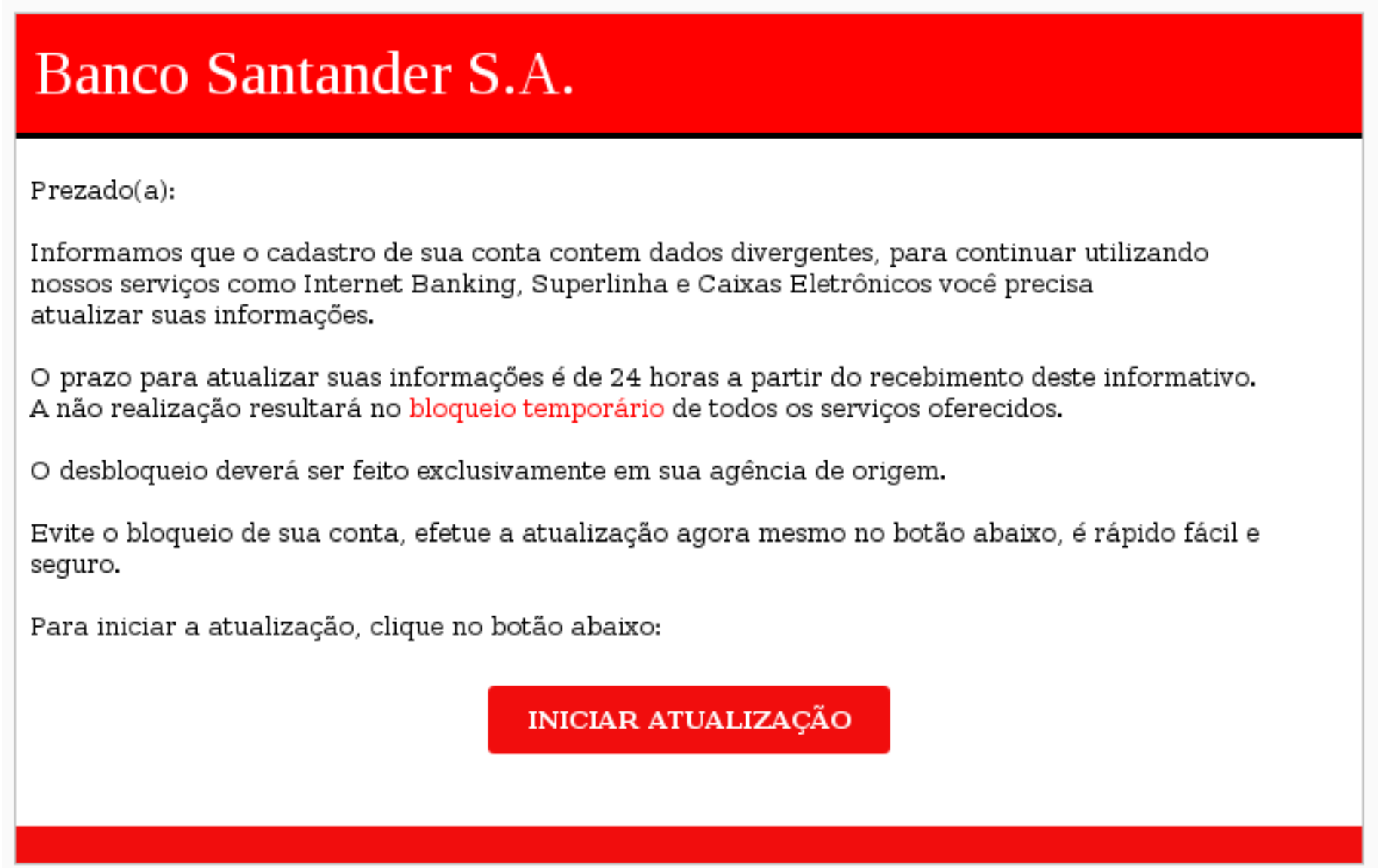
: INTIMAÇÃO ID:	-	Atualizado.
: PROCESSO Nº :	-	907617823M
: PRECENÇA IT :	-	Desabilitado.

< tr>

ANEXO INTIMAÇÃO-MPF (722kb)

ANEXO DOWNLOAD : INTIMAÇÃO-MPF.PDF (722kb)

Entidade Confiável



Banco Santander S.A.

Prezado(a):

Informamos que o cadastro de sua conta contem dados divergentes, para continuar utilizando nossos serviços como Internet Banking, Superlinha e Caixas Eletrônicos você precisa atualizar suas informações.

O prazo para atualizar suas informações é de 24 horas a partir do recebimento deste informativo. A não realização resultará no bloqueio temporário de todos os serviços oferecidos.

O desbloqueio deverá ser feito exclusivamente em sua agência de origem.

Evite o bloqueio de sua conta, efetue a atualização agora mesmo no botão abaixo, é rápido fácil e seguro.

Para iniciar a atualização, clique no botão abaixo:

INICIAR ATUALIZAÇÃO

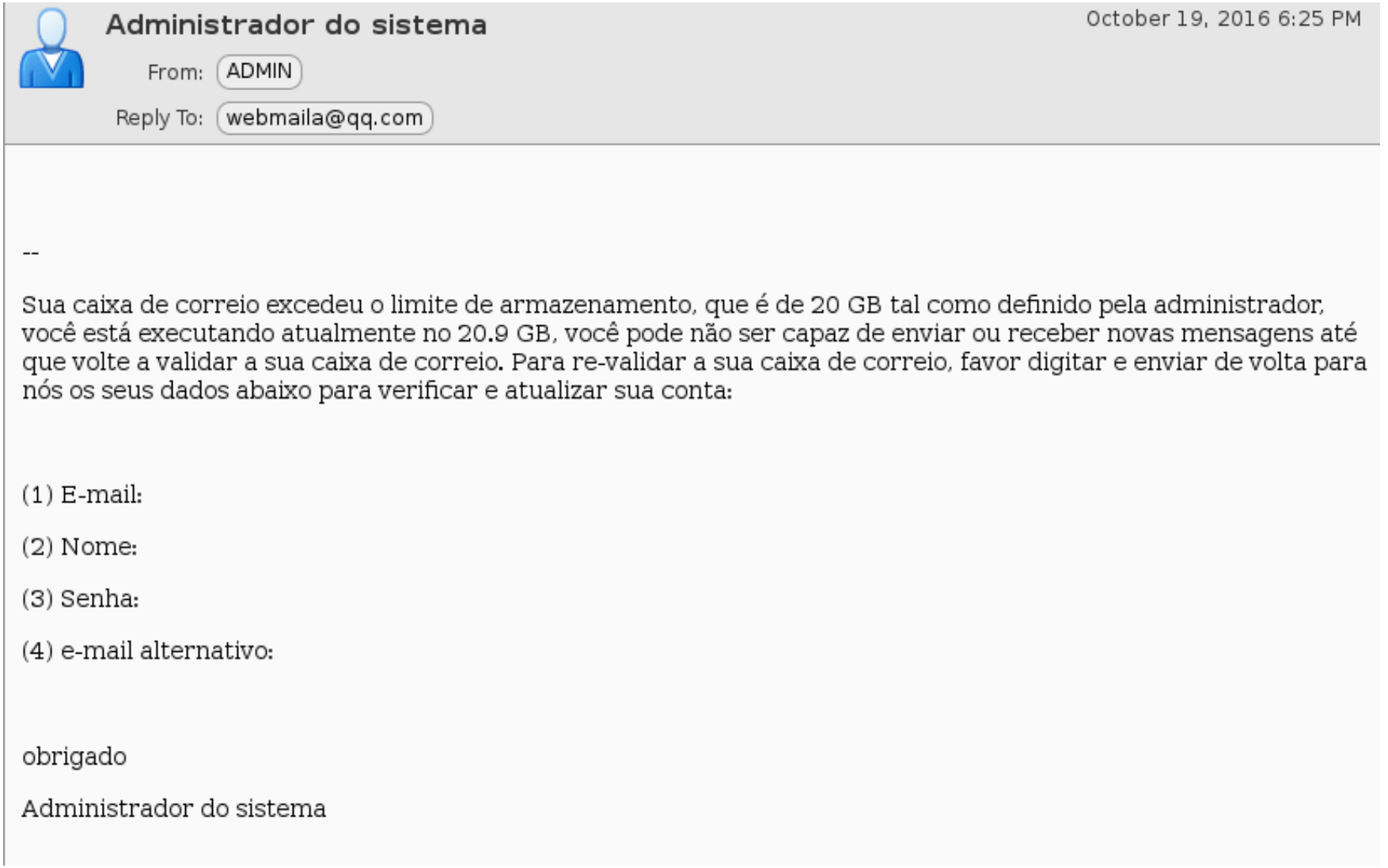
Entidade Confiável

- Phishings enviados por contatos conhecidos que possuem ou utilizaram máquinas infectadas.

- Se tiver algo estranho consultar o remetente da mensagem.

Sentimento de Urgência

Sentimento de Urgência



Administrador do sistema

October 19, 2016 6:25 PM

From: ADMIN

Reply To: webmaila@qq.com

--

Sua caixa de correio excedeu o limite de armazenamento, que é de 20 GB tal como definido pela administrador, você está executando atualmente no 20.9 GB, você pode não ser capaz de enviar ou receber novas mensagens até que volte a validar a sua caixa de correio. Para re-validar a sua caixa de correio, favor digitar e enviar de volta para nós os seus dados abaixo para verificar e atualizar sua conta:

(1) E-mail:

(2) Nome:

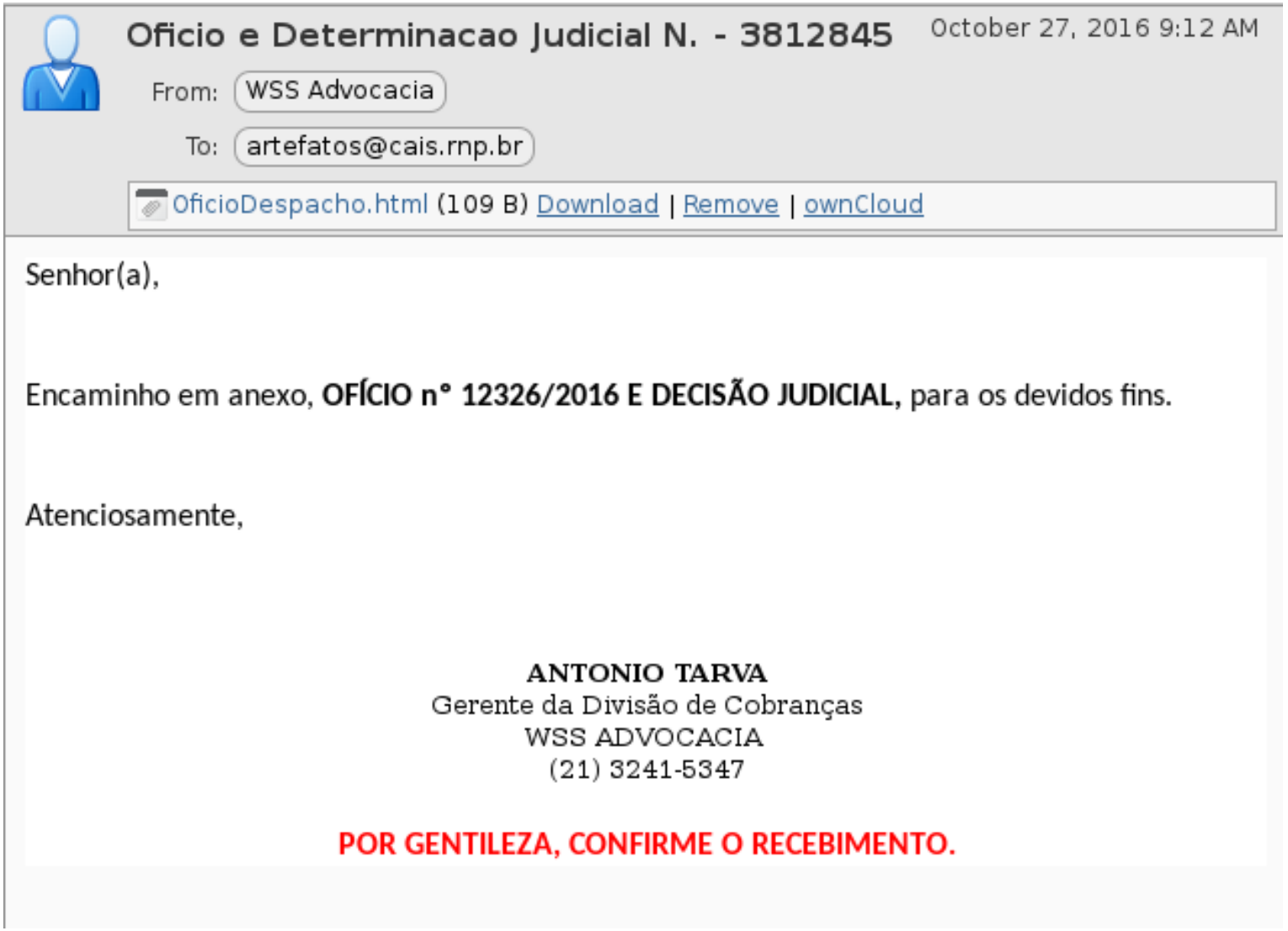
(3) Senha:

(4) e-mail alternativo:

obrigado

Administrador do sistema

Sentimento de Medo e Preocupação



Oficio e Determinacao Judicial N. - 3812845 October 27, 2016 9:12 AM

From: WSS Advocacia

To: artefatos@cais.rnp.br

OficioDespacho.html (109 B) Download | Remove | ownCloud

Senhor(a),

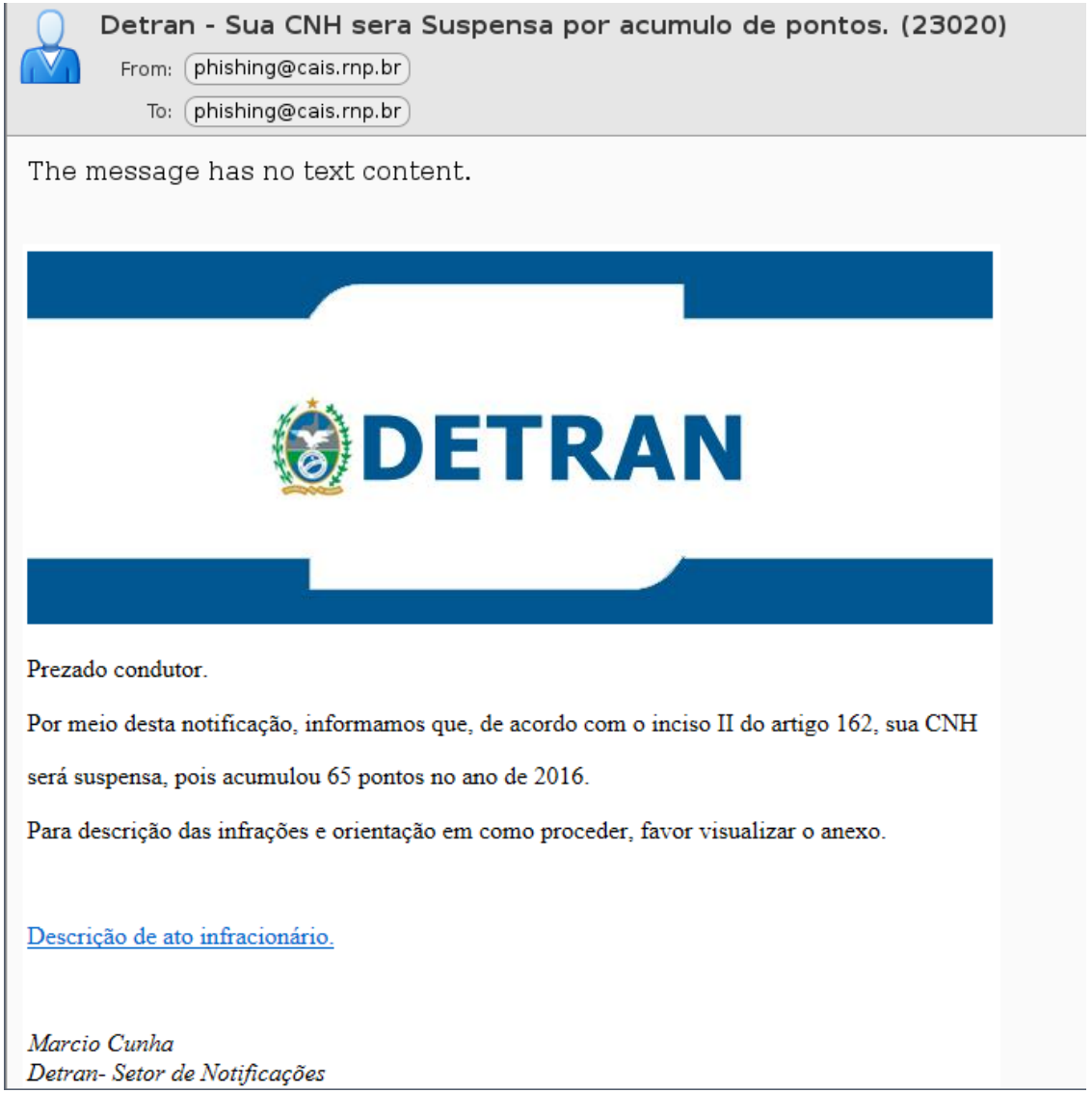
Encaminho em anexo, **OFÍCIO n° 12326/2016 E DECISÃO JUDICIAL,** para os devidos fins.

Atenciosamente,

ANTONIO TARVA
Gerente da Divisão de Cobranças
WSS ADVOCACIA
(21) 3241-5347

POR GENTILEZA, CONFIRME O RECEBIMENTO.

Sentimento de Medo e Preocupação



Detran - Sua CNH sera Suspensa por acumulo de pontos. (23020)

From: phishing@cais.rnp.br

To: phishing@cais.rnp.br

The message has no text content.

DETRAN

Prezado condutor.

Por meio desta notificação, informamos que, de acordo com o inciso II do artigo 162, sua CNH será suspensa, pois acumulou 65 pontos no ano de 2016.

Para descrição das infrações e orientação em como proceder, favor visualizar o anexo.

Descrição de ato infracionário.

Marcio Cunha
Detran- Setor de Notificações

Sentimento de Medo e Preocupação

SOU UM AMIGO SEU

Não vou me identificar, mas sou um amigo, isso e apenas um aviso, você esta sendo traido não tive a coragem de te contar pessoalmente mas como imagens falam mais que mil palavras, então resolvi te enviar essas fotos como prova do que esta acontecendo...

Meu conselho é que olhe as fotos

Esta Mensagem esta contida com o mais sigiloso conteúdo!

Sentimento de Curiosidade

Sentimento de Curiosidade

VIDEO E FOTOS DO ACIDENTE DE CRISTIANO ARAUJO (CONFIRA) July 2, 2015 7:41 PM

From: NOTICIA

To: Recipients

A Policia Civil de Goiás indica duas pessoas pelo vazamento de vídeo e imagens relacionados a **Morte de Cristiano Araujo**, que morreu em um acidente de carro na BR-153 em Goiás, o cantor sertanejo estava sendo preparado para o sepultamento quando foi filmado pelos funcionários.Segundo informações, os funcionários irão responder pelo crime de vilipendiar cadáver(desrespeitar o corpo do Falecido) ,com a pena que vai até 3 anos de prisão.

Segundo informações, são dois funcionários da Clinica Oeste, entre elas uma terceira pessoa,cujo divulgou as imagens para as redes sociais, ele(a) poderá ser indiciado também.

Segundo Marcia, funcionaria que estava fazendo a filmagem, Marco só percebeu que estava sendo gravado quando o vídeo já estava se passando pela metade, que não fez nenhum argumento sobre parar de filmar, que

Vantagem Financeira

Caso não esteja visualizando as imagens, acesse aqui

~~LOJAS AMERICANAS~~

Smart TV Nano Cristal 50" Samsung 50JS7200 SUHD 4K com Conversor Digital 4 HDMI 3 USB Wi-Fi FunÃ§Ã£o Games Quad Core (codigo do produto: 117185854)

Sul e Sudeste

últimas unidades!

~~R$ 3.685,97~~ - **(mais de 70% de desconto)**

comprar

R$ 1.260,00

Promoção valida apenas para pagamento via BOLETO.

FRETE GRATÍS TODO PAÃS

Vantagem Financeira

NETFLIX

NETFLIX: Assista 3 meses gr�tis. Apenas R$1,90 depois que sua utiliza��o gratuita terminar.

Promo��o de Estr�ia de novos filmes e series.

3 meses gr�tis, por apenas R$1,90 ao final de seu terceiro m�s! loucura n�?

A sua tela e nosso cinema. Vamos !

Vamos l� ►

Agradecemos pela aten��o

�Seus amigos da Netflix

Perda Financeira

Comunicado Importante Bradesco.

Prezado Cliente,

Informamos que seu dispositivo de segurança contendo suas chaves ou tokens de acesso, encontra-se vencido e por medidas de segurança deve ser reativado, evitando assim, o bloqueio temporário de sua conta aos canais de auto-atendimento (**Caixas eletrônicos, InternetBanking e Smartphones**). Caso a reativação não seja efetuada, conforme a errata nº 17619BR, cobranças poderão ser geradas nos valores entre **R$120,00** e **R$134,48** para reativar seu dispositivo de acesso atual - **Cartão de segurança, TOKEN via chaveiro ou TOKEN em dispositivo móvel.**

A atualização cadastral (recadastramento) é obrigatório.

ATENÇÃO: este processo é obrigatório e caso nosso sistema não identifique este procedimento no prazo de 24 horas, seu acesso será bloqueado temporariamente por questões de segurança com desbloqueio previsto somente para sua agência de origem, mediante apresentação de documentação comprobatória de identidade.

Clique no botão "**Confirmar Atualização**" para aderir ao processo de atualização.

Confirmar Atualização

Caso o botão não funcione **clique aqui**.

© Banco Bradesco SA - CNPJ: 60.746.948.0001-12
Alô Bradesco - 0800 704 8383 |Ouvidoria - 0800 727 9933.

Truques Tecnológicos

Falso Remetente

Return-Path: root@underconto.carvalhoassessoria.com
Received: from mail.pop-ba.rnp.br (LHLO mail.pop-ba.rnp.br)
(2801:86:0:4:0:0:0:27) by mail.pop-ba.rnp.br with LMTP; Tue, 11 Oct 2016
03:09:17 -0300 (BRT)
Received: from localhost (localhost [IPv6:::1])
by mail.pop-ba.rnp.br (Postfix) with ESMTP id B70F1AC0C30
for <fraudes@pop-ba.rnp.br>; Tue, 11 Oct 2016 03:09:17 -0300 (BRT)
[...]
Received: from NY1ZXGVCV111101.local (underconto.carvalhoassessoria.com [74.201.232.112])
by mx0.rnp.br (8.14.4/8.14.4/Debian-8) with ESMTP id u9B69Ej8002706
for <artefatos@cais.rnp.br>; Tue, 11 Oct 2016 03:09:14 -0300
Received: by NY1ZXGVCV111101.local (Postfix, from userid 0)
id 33B9ECF24C; Tue, 11 Oct 2016 04:54:50 +0000 (UTC)
content-type: text/html
Subject: Ultimo aviso: Atualizacao de Seguranca Obrigatoria
From: Banco do Brasil <sac@bbauto.com>
To: artefatos@cais.rnp.br
Message-Id: <20161011052721.33B9ECF24C@NY1ZXGVCV111101.local>
Date: Tue, 11 Oct 2016 04:54:50 +0000 (UTC)

Truques Tecnológicos

- Mensagens com arquivos em anexo
  - Extensão dos arquivos
  - Documentos com macros
  - Arquivos compactados com senha

- Mensagens com URLs
  - Utilizada em 90% das fraudes atuais
  - Deixa o tamanho da mensagem menor
  - Mais fácil de manipular: HTML tag, DNS, HTTP Redirect

Simulação de Domínio Válido

- Domínios parecidos com os verdadeiros
  - Adição/Remoção de uma letra
- Uso de sub-domínios
  - http://extra.br.com
- Menção à marca no domínio
  - http://promocaodacielo.com
  - http://blackfridaylojasamericanas.com

Simulação de Domínio Válido

- Maioria dos domínios das fraudes brasileiras é .com

Domínio	Quantidade
com	727
br	183
net	45
org	40
pl	21
ru	20
co	18
info	12
me	12
lt	9

Fonte: https://cauma.pop-ba.rnp.br/

Simulação de Domínio Válido

Santander

Corre��es importantes

Prezado Cliente(a):

Informamos que desde o dia 20/10/2016 nosso sistema de identifica��o mudou, para garantir melhor acesso a sua conta atrav�s do (Internet Banking, Telefone, Caixa Eletr�nico), E ser� necess�rio realizar uma corre��o em seus dados cadastrais.

Sob cl�usula 12.288/908, do c�digo de privacidade do Banco Santander, todos os correntistas ter�o seus certificados de seguran�a definidos automaticamente.

! Para corrigir sua conta, basta clicar no link abaixo e seguir os passos.

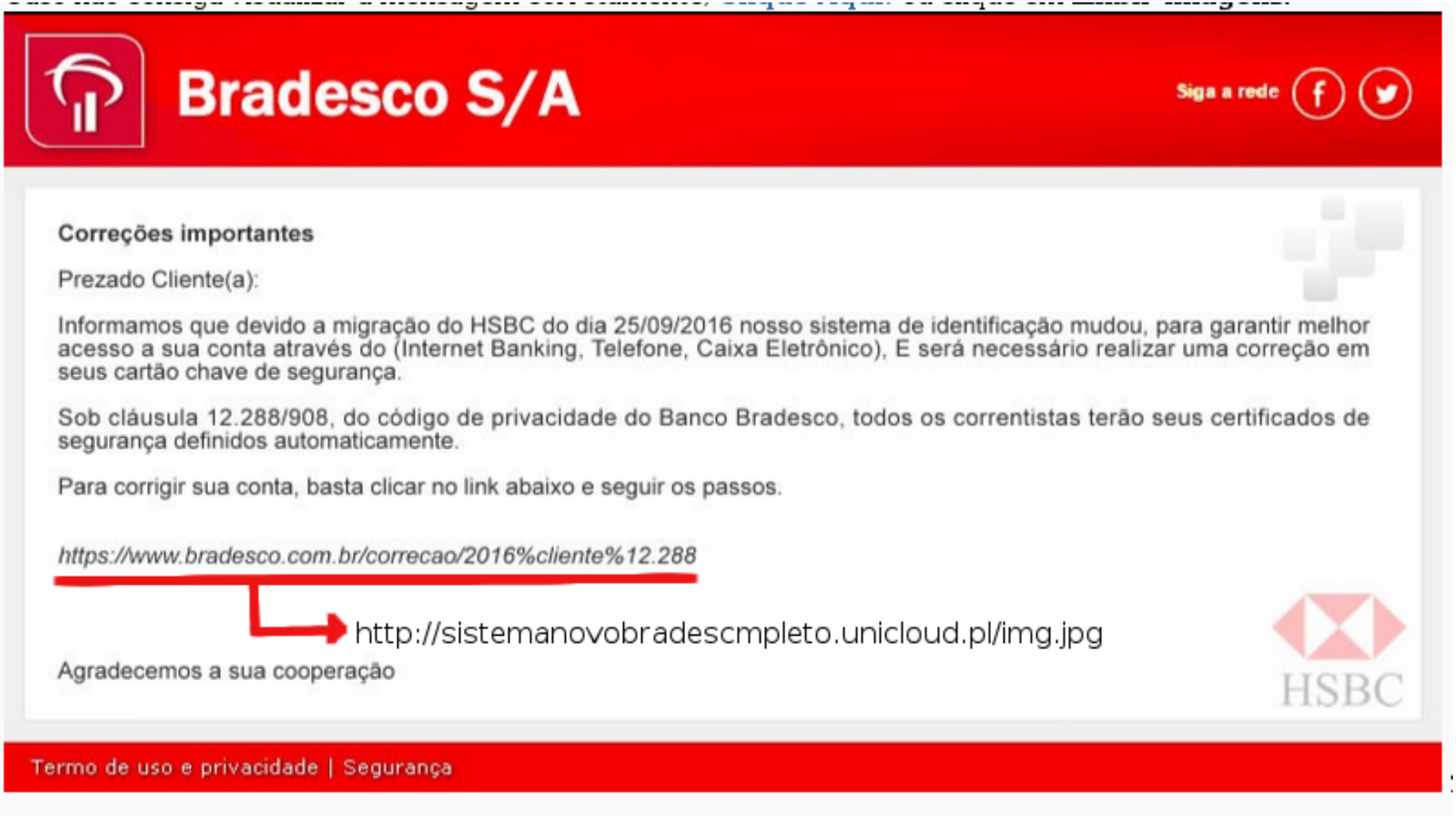
https://www.santander.com.br/correcao/2016%cliente%12.288

http://carvalhoassessoria.com/atendimento_pessoa_fisica...

agradecemos a sua coopera��o

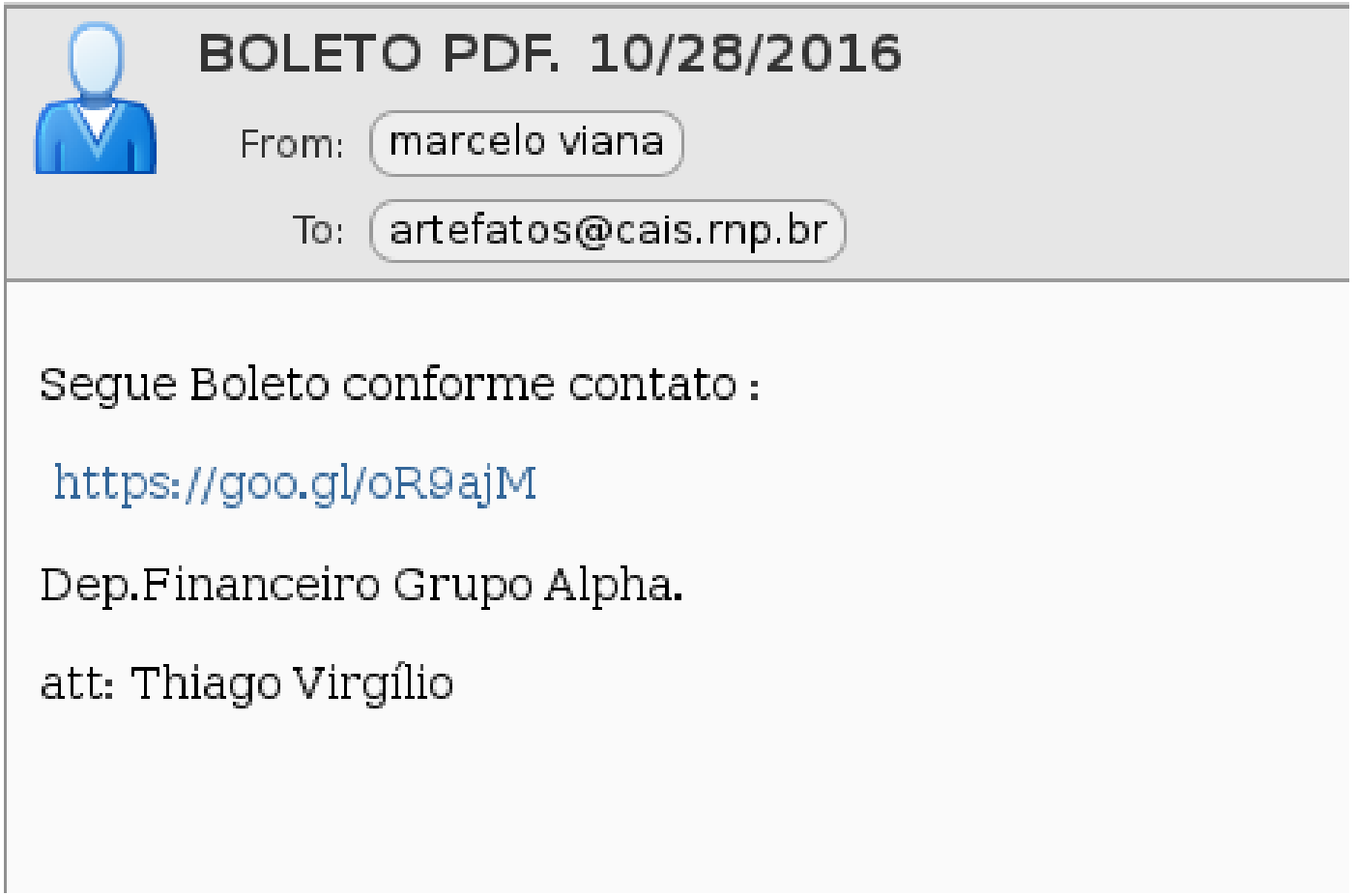
CNPJ: 90.400.888/0001-42 Avenida Presidente Juscelino Kubitschek, 2235 - Bloco A, Vila Ol�mpia, S�o Paulo/SP - CEP 04543-011.

Simulação de Domínio Válido



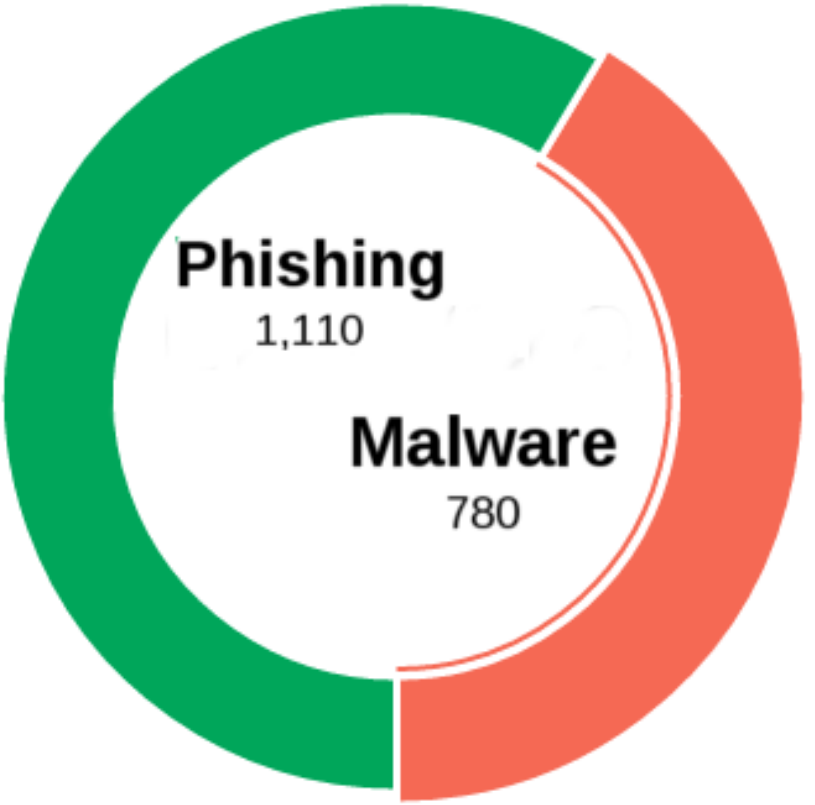
Simulação de Domínio Válido

Serviços de Encurtador de URLs



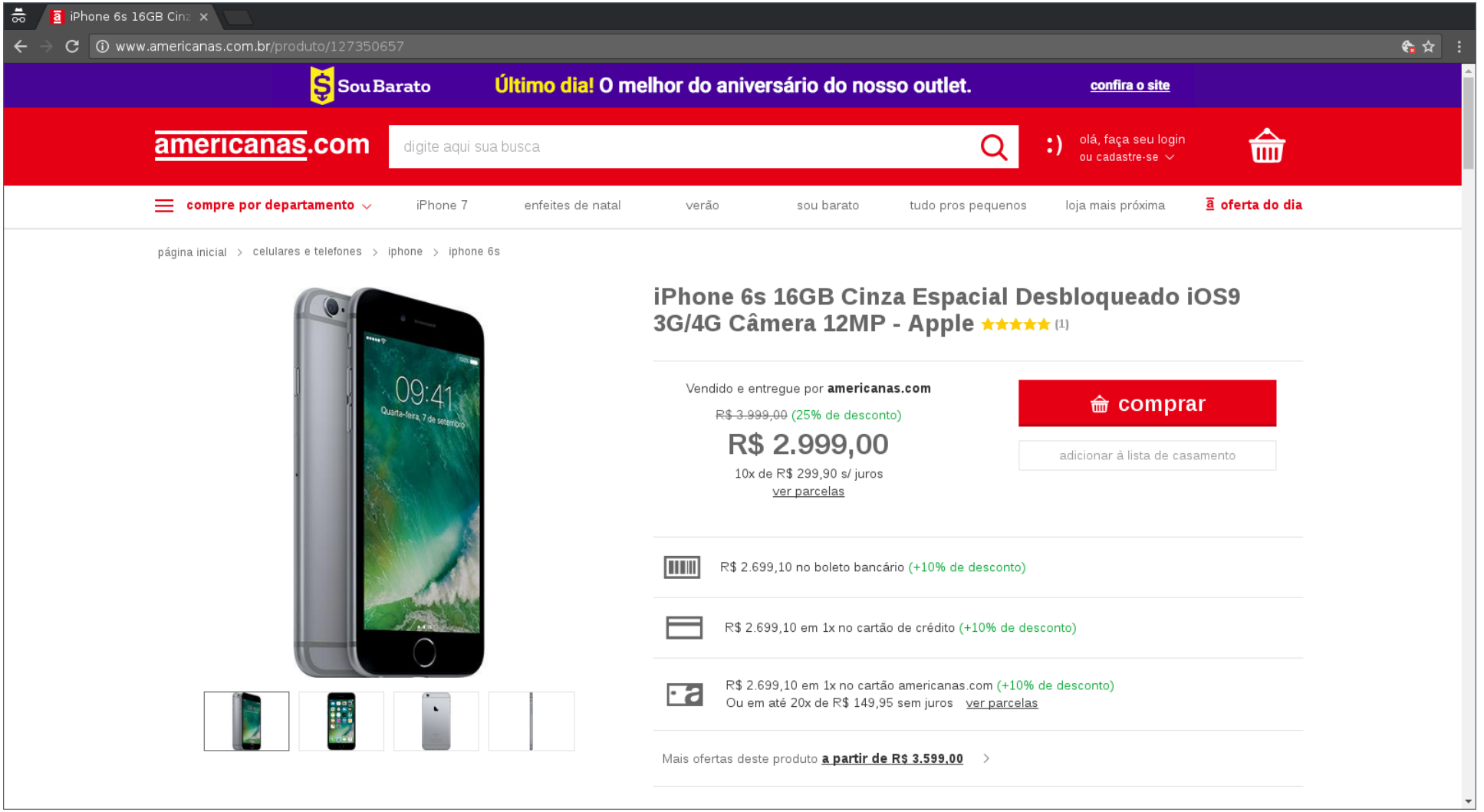
Consequências dos Phishings

- Induz o usuário a:
  - Fornecer informações



Fonte: https://cauma.pop-ba.rnp.br/url/statistics

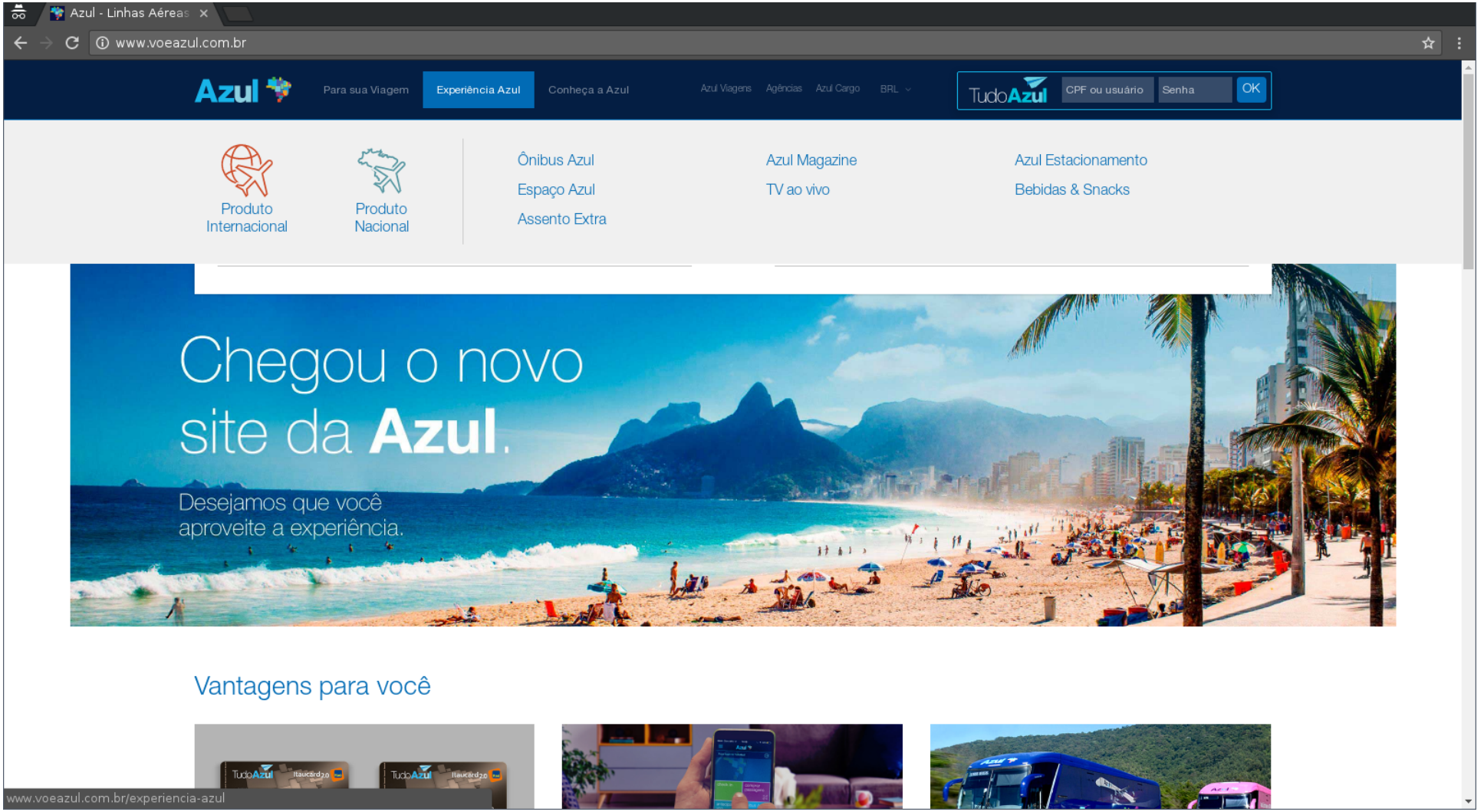
Site Verdadeiro



Site Falso


iPhone 6s 16GB Cinz
65.181.112.117/www.americacanas.com.br/produto/4259005347266/iphone-6s-16GB-cinza-espacial-tela-5.5-ios-9-4g-camera-12MP-apple
televendas 24h
atendimento
meus pedidos
minha conta
loja mais próxima
cartão americanas.com
Seu Barato
O maior outlet da internet
americanas.com
a maior loja. os menores preços.
buscar
olá ,
sair
minha cesta
1 item
compre por departamento
dia das crianças
melhores ofertas
organização
iPhone em oferta
oferta do dia
saldão
O maior e mais completo do Brasil.
celulares e telefones
iphone
iphone 6s plus
iPhone 6s 16GB Cinza Espacial Desbloqueado iOS9 3G/4G Câmera 12MP - Apple
(código do produto: 120998872)
(5 avaliações)
avalie este produto
zoom
passe o mouse
veja a regra
R$ 3.799,00 - (desconto de 50%)
R$ 1.899,50
Promoção valida apenas para pagamento via BOLETO
Boleto
lista casamento
recomendar
últimas unidades
vendido e entregue por americanas.com
comprar
outras opções de compra
carioca celulares
R$ 3.799,00 em até 6x
comprar
Preencha esse campo com um CEP válido.
frete e prazo:
CEP
calcular
não sei meu CEP
Preencha esse campo com um CEP válido.
até 80% de desconto + até 12%* de desconto em 1X no cartão
*confira as regras.
informações técnicas
compre junto
avaliação dos clientes
garantia estendida
javascript:;

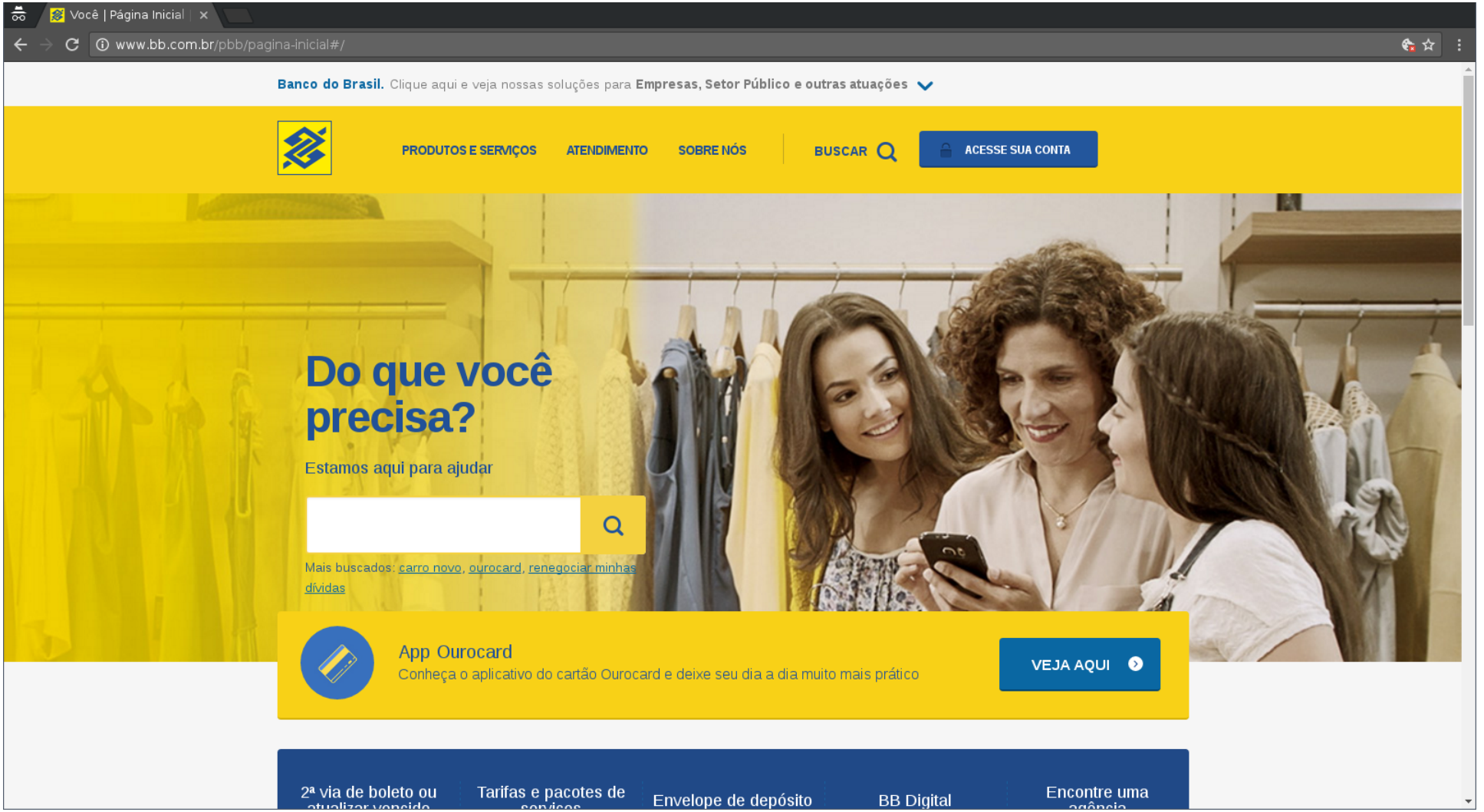
Site Verdadeiro



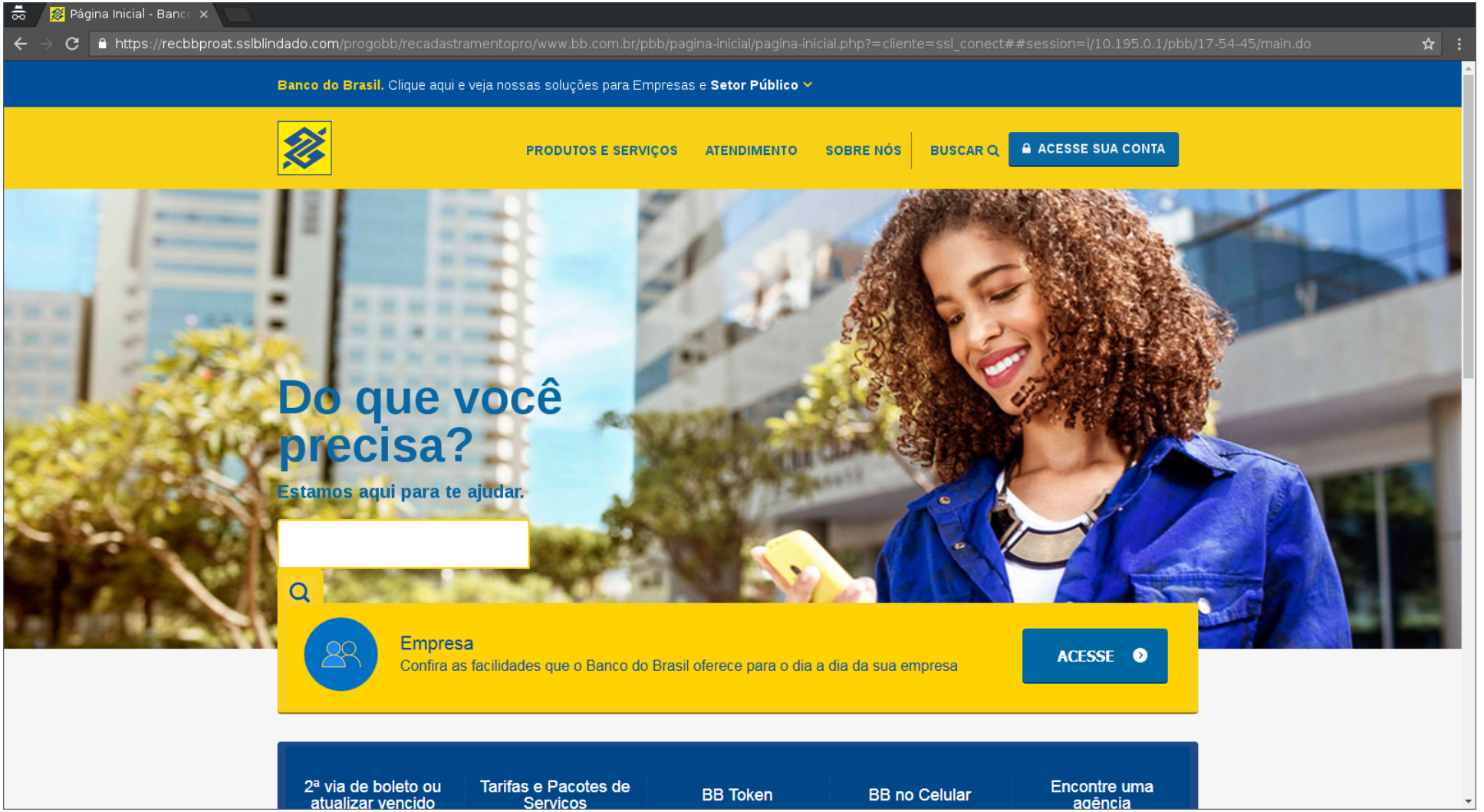
Site Falso


azulnewspromo.ddns
azulnewspromo.ddns.net/tudoazul/84IyPmJTnN
Azul
comprar Passagem
minhas Reservas
conheça a Azul
TudoAzul
Programa de Vantagens
Bem-vindo ao TudoAzul
o seu Programa de Vantagens.
Logar no Tudo Azul
Cadastre-se no Tudo Azul
VISA + MasterCard + Azul Linhas Aéreas Brasileiras = usou Voou
TudoAzul
Programa de Vantagens
Acumule pontos utilizando seu cartão Visa ou Mastercard.
Faça seu cadastro, comece a acumular pontos e troque por passagens aéreas.
Cadastro Rápido
*Preenchimento obrigatório
Nome* (como está em seu cartão)
Número do cartão de crédito* (Visa ou Mastercard)
Validade*
CVV*
CPF* (será seu login no Tudo Azul)
E-mail*
Senha*
Confirmação de senha*
Ver Regras do Programa
Não concordo
CADASTRAR (Aceito as regras)

Site Verdadeiro

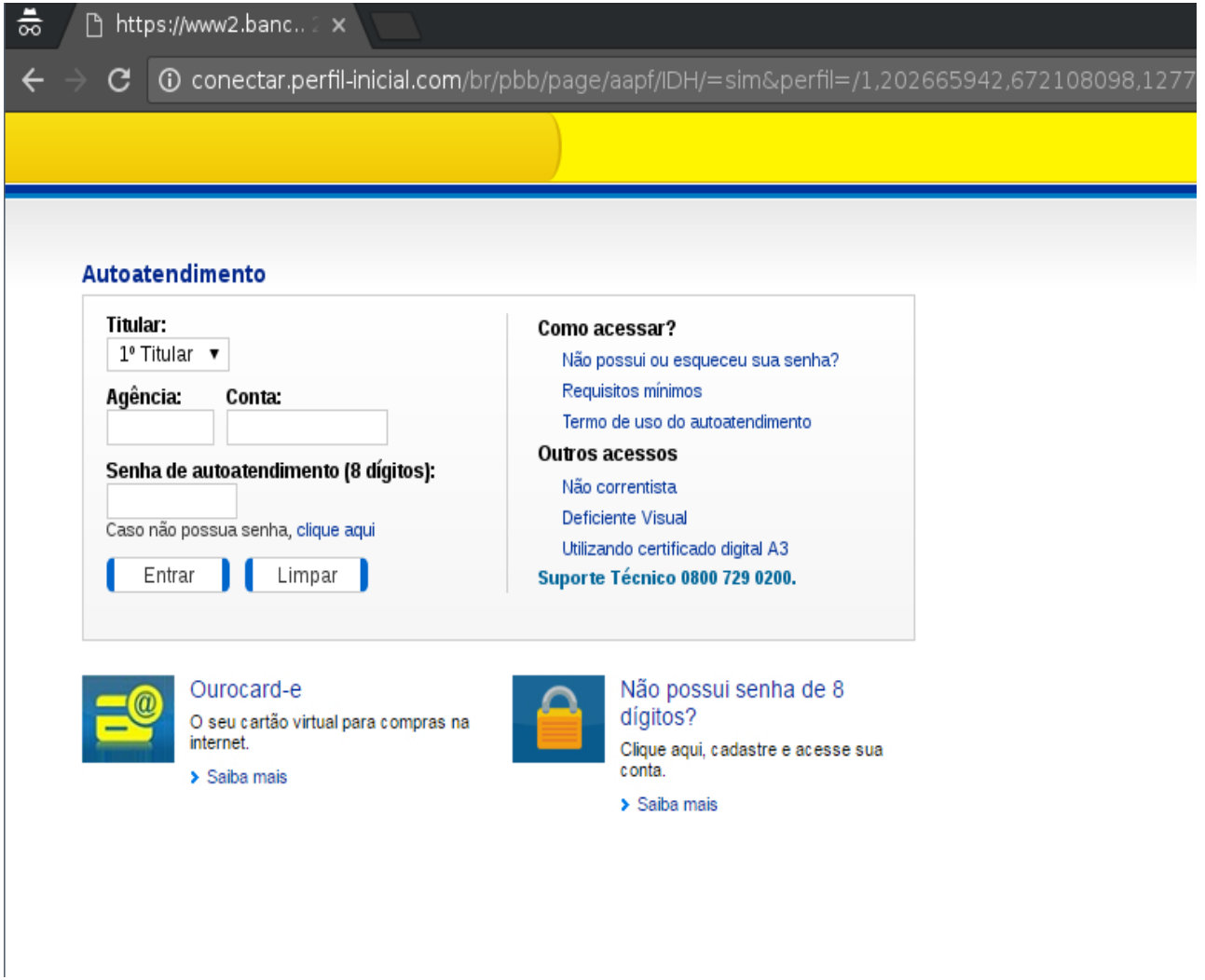


Site Falso


Página Inicial - Banco
https://recbbproat.sslblindado.com/progobb/recadastramentopro/www.bb.com.br/pbb/pagina-inicial/pagina-inicial.php?=cliente=ssl_conect##session=i/10.195.0.1/pbb/17-54-45/main.do
Banco do Brasil. Clique aqui e veja nossas soluções para Empresas e Setor Público
PRODUTOS E SERVIÇOS
ATENDIMENTO
SOBRE NÓS
BUSCAR
ACESSE SUA CONTA
Do que você precisa?
Estamos aqui para te ajudar.
Empresa
Confira as facilidades que o Banco do Brasil oferece para o dia a dia da sua empresa
ACESSE
2ª via de boleto ou atualizar vencido
Tarifas e Pacotes de Serviços
BB Token
BB no Celular
Encontre uma agência

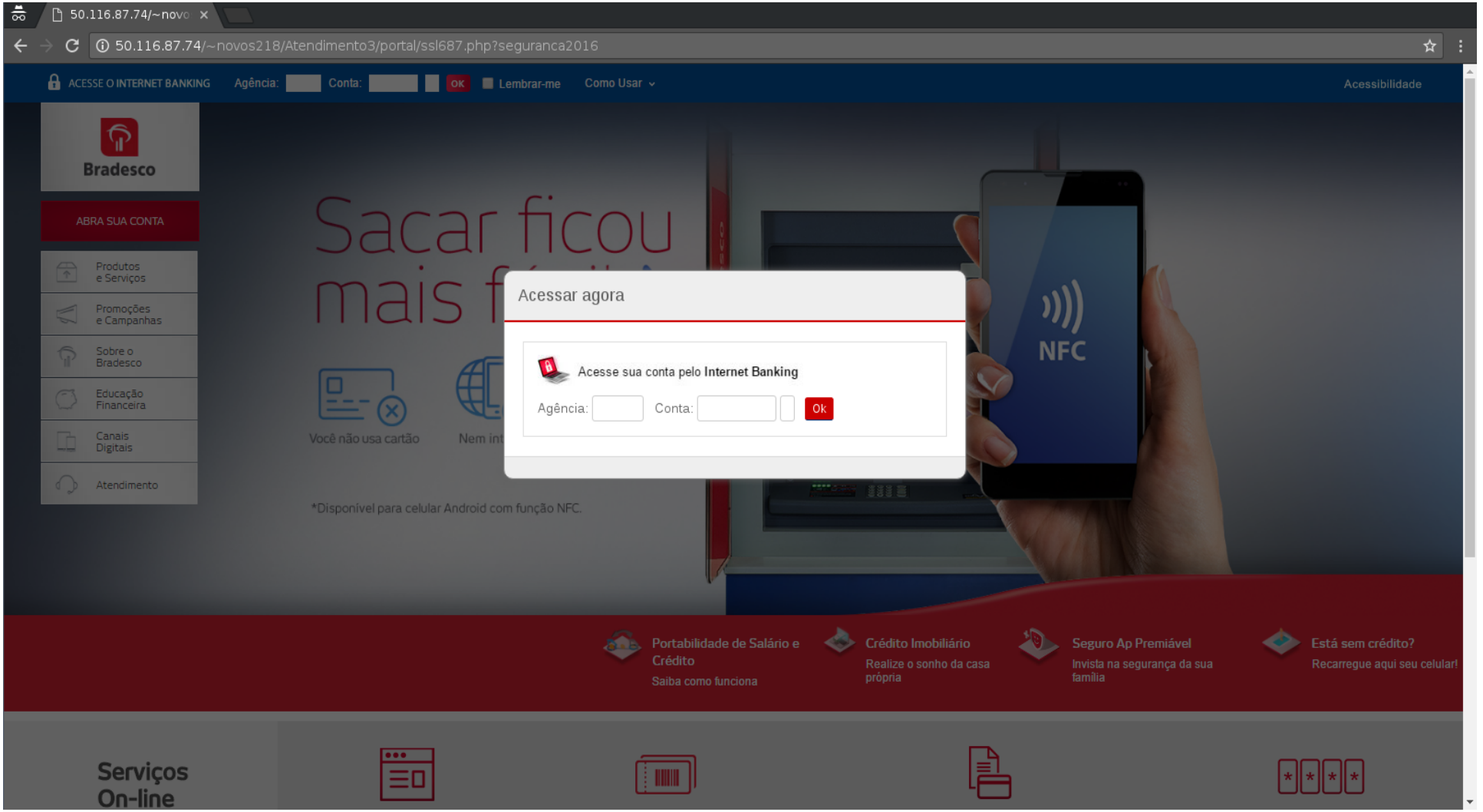
Site Verdadeiro

Site Falso

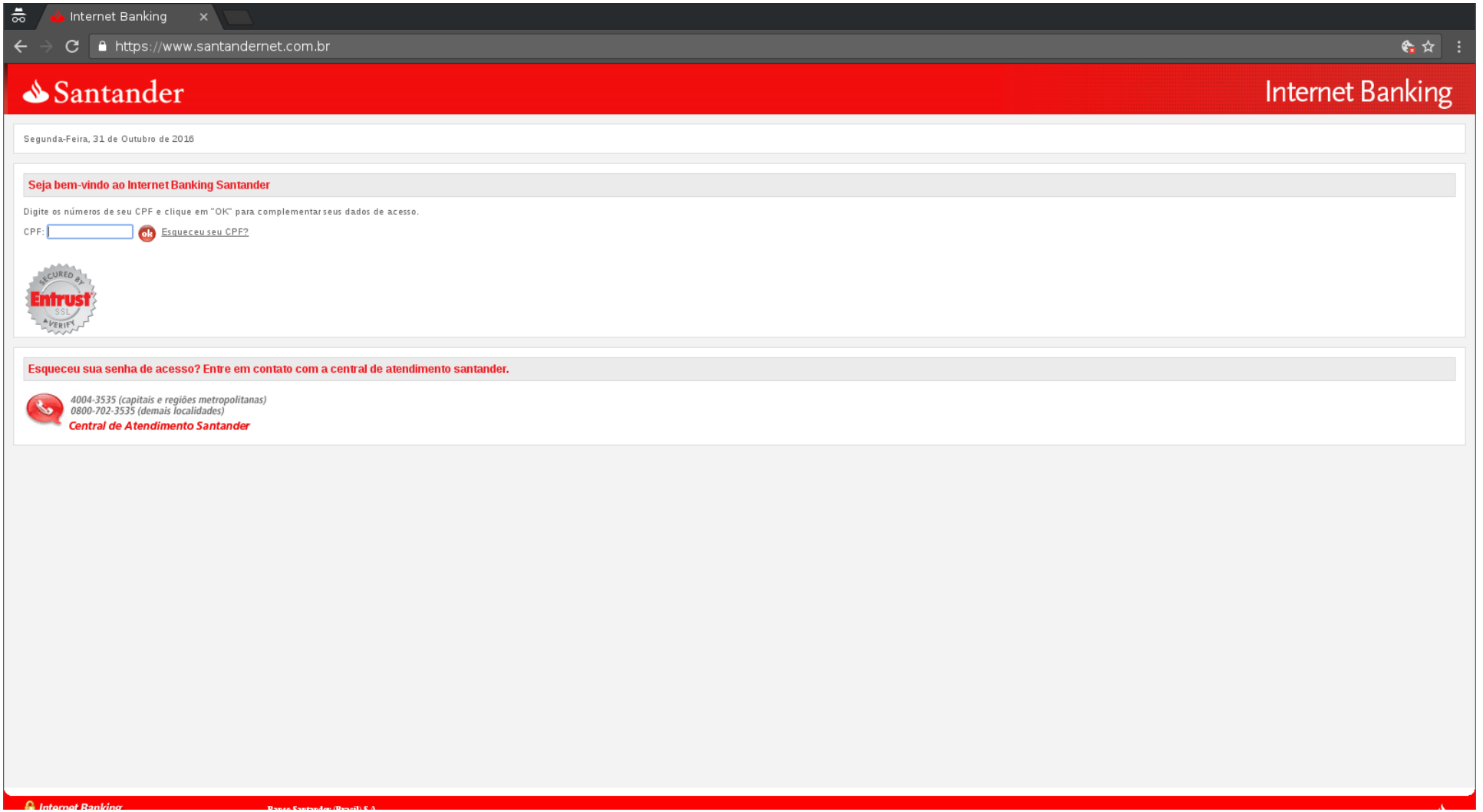

https://www2.banc..
conectar.perfil-inicial.com/br/pbb/page/aapf/IDH/=sim&perfil=/1,202665942,672108098,1277
Autoatendimento
Titular:
1º Titular
Agência:
Conta:
Senha de autoatendimento (8 dígitos):
Caso não possua senha, clique aqui
Entrar
Limpar
Como acessar?
Não possui ou esqueceu sua senha?
Requisitos mínimos
Termo de uso do autoatendimento
Outros acessos
Não correntista
Deficiente Visual
Utilizando certificado digital A3
Suporte Técnico 0800 729 0200.
Ourocard-e
O seu cartão virtual para compras na internet.
Saiba mais
Não possui senha de 8 dígitos?
Clique aqui, cadastre e acesse sua conta.
Saiba mais

Site Verdadeiro

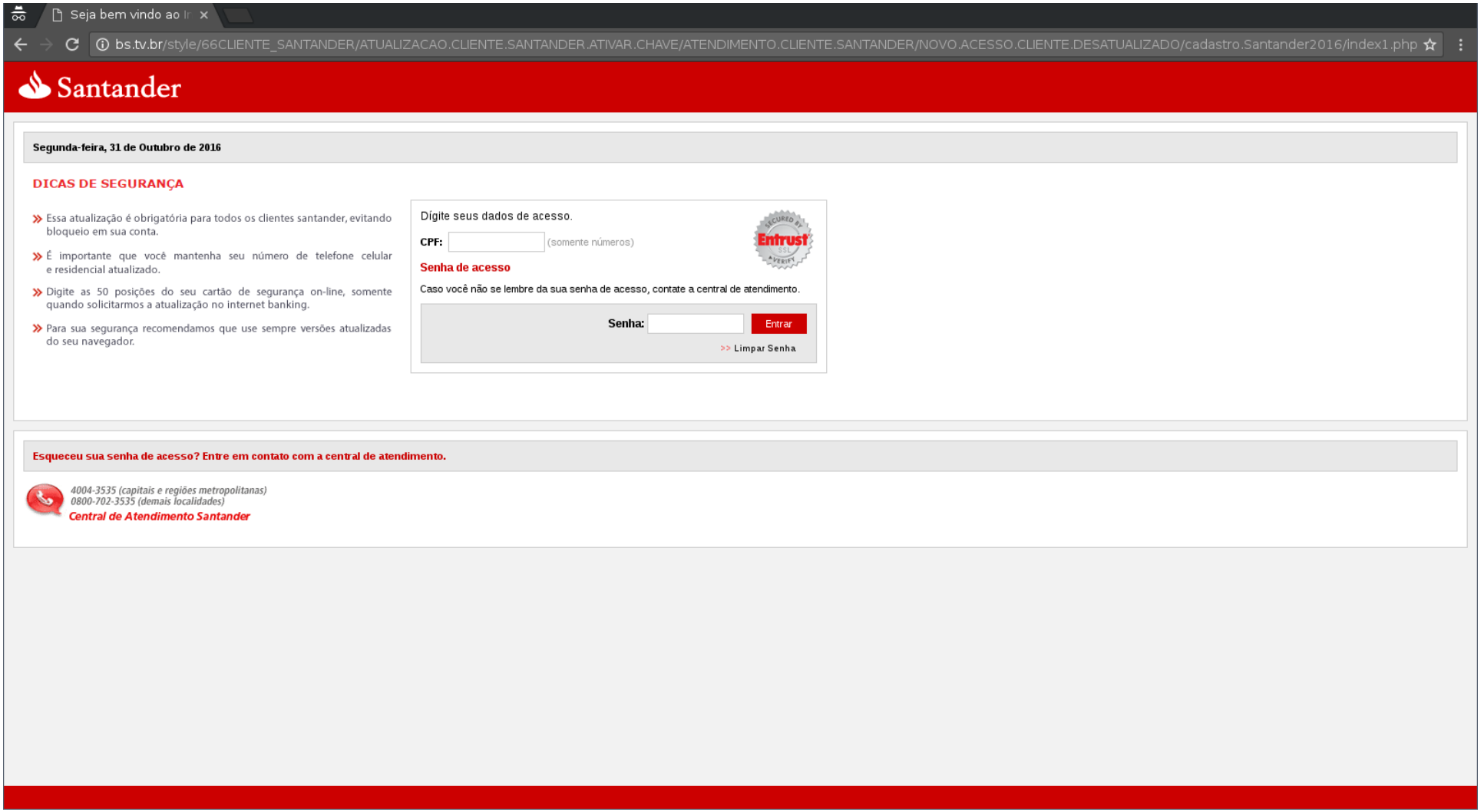
Site Falso


50.116.87.74/~novo
50.116.87.74/~novos218/Atendimento3/portal/ssl687.php?seguranca2016
ACESSE O INTERNET BANKING
Agência:
Conta:
OK
Lembrar-me
Como Usar
Acessibilidade
Bradesco
ABRA SUA CONTA
Produtos e Serviços
Promoções e Campanhas
Sobre o Bradesco
Educação Financeira
Canais Digitais
Atendimento
Sacar ficou
Você não usa cartão
*Disponível para celular Android com função NFC.
Acessar agora
Acesse sua conta pelo Internet Banking
Agência:
Conta:
Ok
NFC
Portabilidade de Salário e Crédito
Saiba como funciona
Crédito Imobiliário
Realize o sonho da casa própria
Seguro Ap Premiável
Invista na segurança da sua família
Está sem crédito?
Recarregue aqui seu celular!
Serviços On-line

Site Verdadeiro

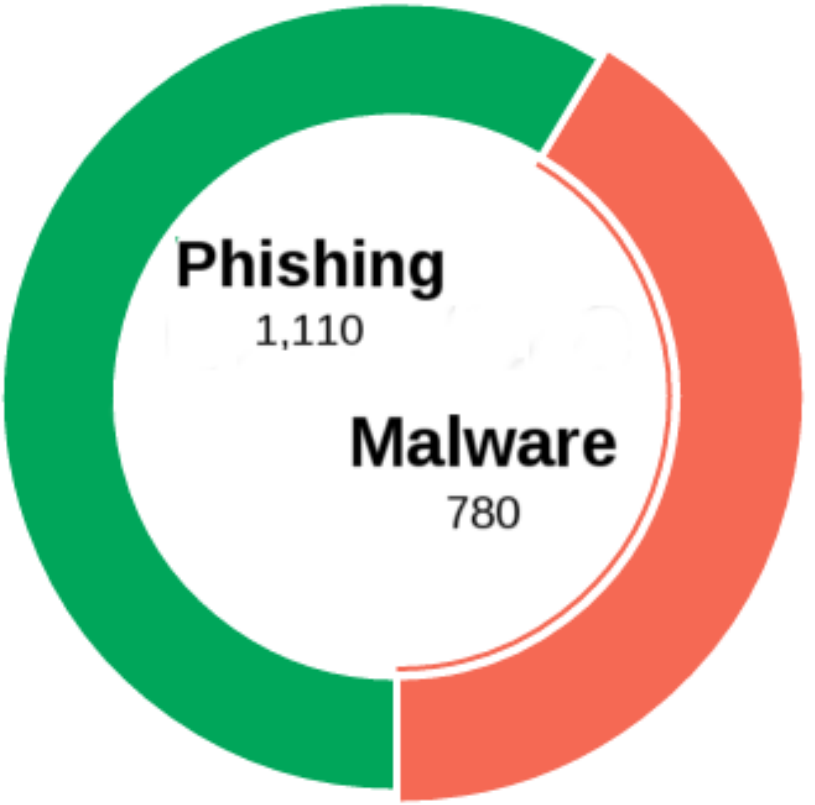


Site Falso


Seja bem vindo ao I
bs.tv.br/style/66CLIENTE_SANTANDER/ATUALIZACAO.CLIENTE.SANTANDER.ATIVAR.CHAVE/ATENDIMENTO.CLIENTE.SANTANDER/NOVO.ACESSO.CLIENTE.DESATUALIZADO/cadastro.Santander2016/index1.php
Santander
Segunda-feira, 31 de Outubro de 2016
DICAS DE SEGURANÇA
Essa atualização é obrigatória para todos os clientes santander, evitando bloqueio em sua conta.
É importante que você mantenha seu número de telefone celular e residencial atualizado.
Digite as 50 posições do seu cartão de segurança on-line, somente quando solicitarmos a atualização no internet banking.
Para sua segurança recomendamos que use sempre versões atualizadas do seu navegador.
Dígite seus dados de acesso.
CPF:
(somente números)
Senha de acesso
Caso você não se lembre da sua senha de acesso, contate a central de atendimento.
Senha:
Entrar
>> Limpar Senha
Esqueceu sua senha de acesso? Entre em contato com a central de atendimento.
4004-3535 (capitais e regiões metropolitanas)
0800-702-3535 (demais localidades)
Central de Atendimento Santander

Consequências dos Phishings

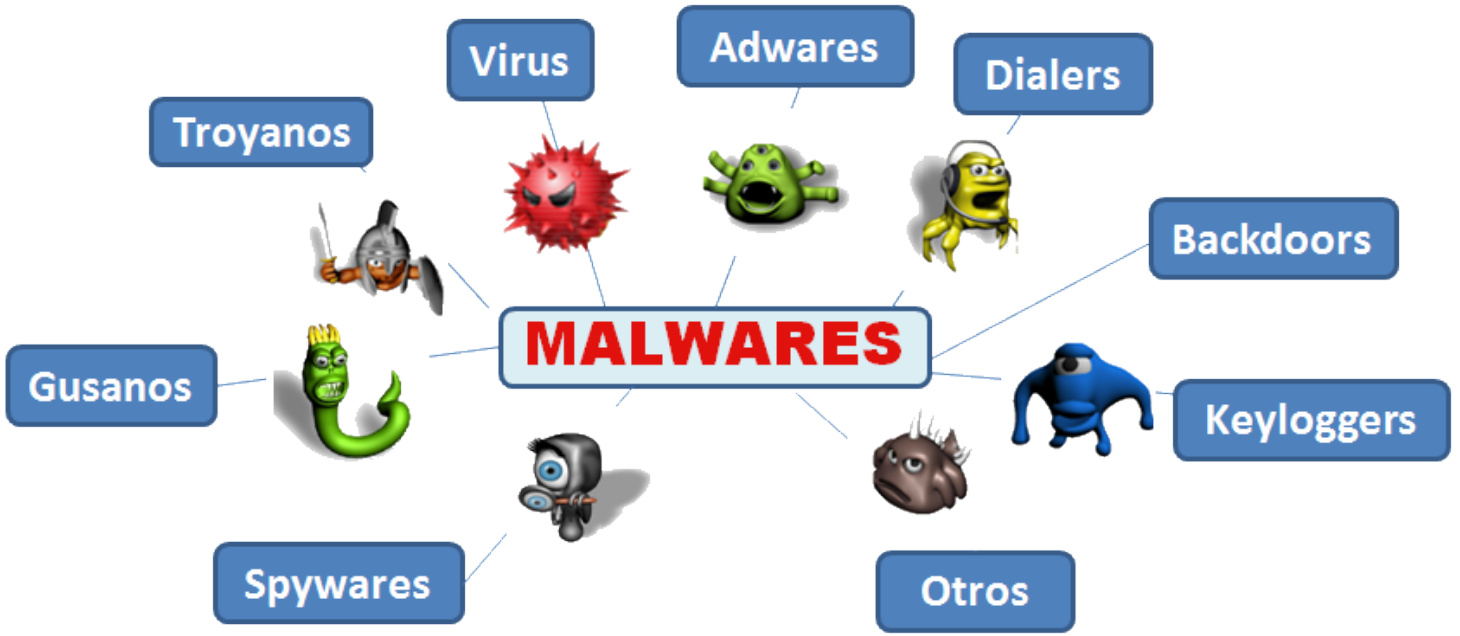
- Induz o usuário a:
  - Fornecer informações
  - Instalar malwares



Fonte: https://cauma.pop-ba.rnp.br/url/statistics

Malware

- É um software destinado a infiltrar-se em sistema de computador alheio de forma ilícita, com o intuito de causar danos, roubar de informações, dentre outras atividades maliciosas.



Malware

- Principais formas de propagação:
  - Exploração de vulnerabilidades
  - Execução de origem desconhecida
  - Através de softwares piratas

Ninguém está a salvo

Ninguém está a salvo

- Sistema de raio-x infectado na UFBA

Ransomware

- Sequestra o dispositivo ou os dados do usuário
  - Arquivos em nuvem não estão seguros
- Exige pagamento (resgate) para desbloquea-los

Evite ser Fisgado

Evite ser Fisgado

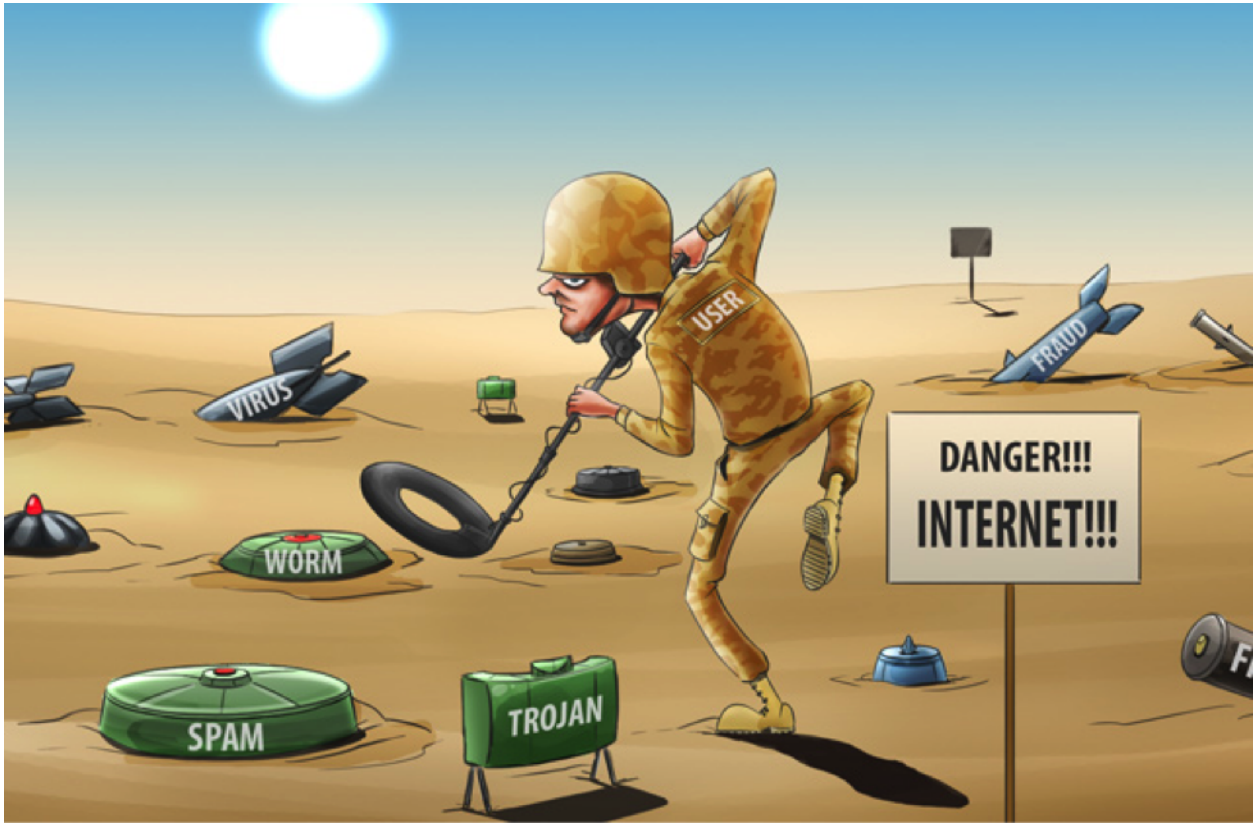
- Não considere uma mensagem confiável baseado no remetente.
- Confirme com o remetente a partir de outro meio de comunicação.

Evite ser Fisgado

- Pense um pouco antes de:
  - Clicar
  - Executar
  - Baixar

Evite ser Fisgado

- “Cuidado por onde você anda...”

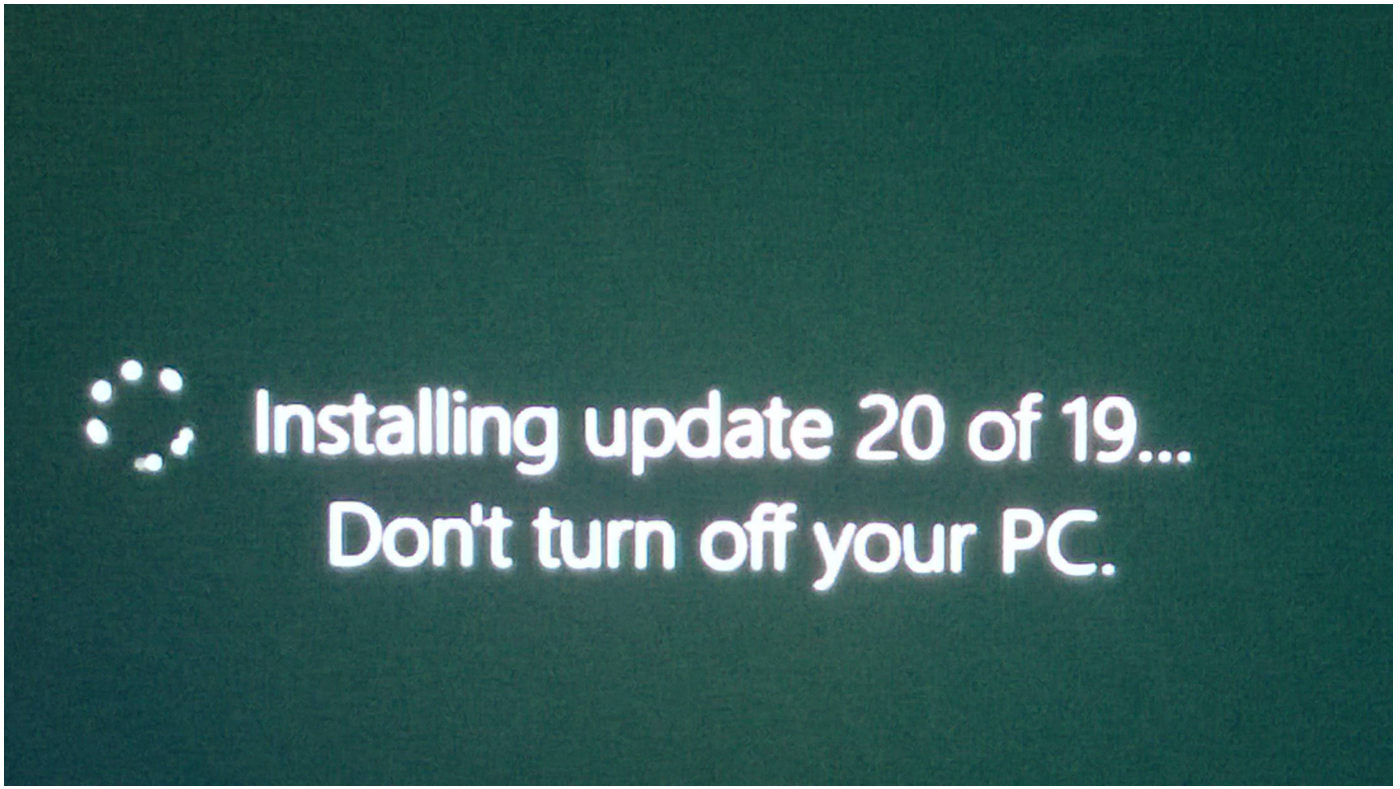


Evite ser Fisgado

- Instalar aplicativos de segurança, mante-los atualizados e fazer uso deles.

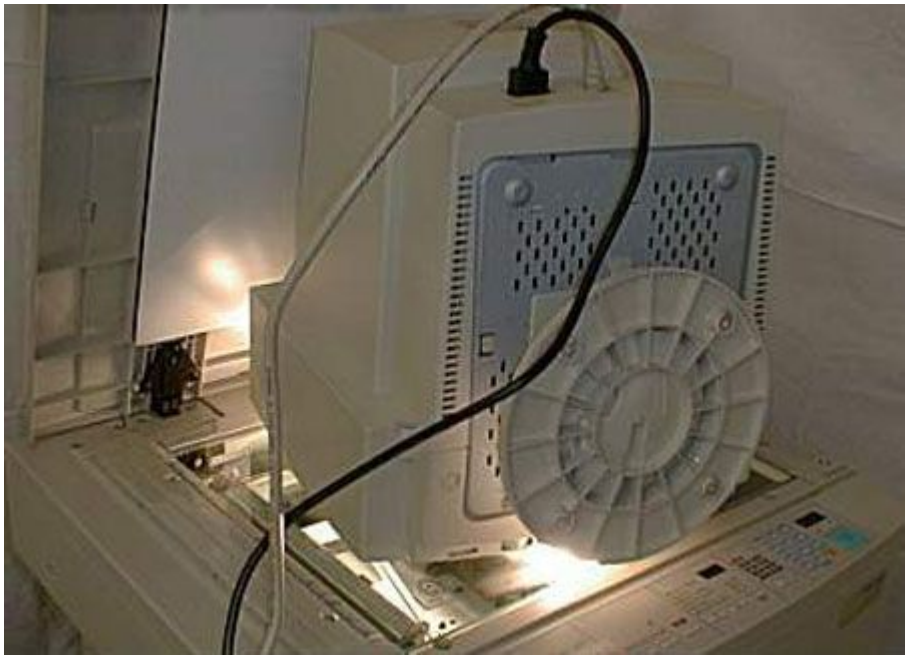
Evite ser Fisgado

- Mantenha o sistema operacional e aplicativos atualizados.

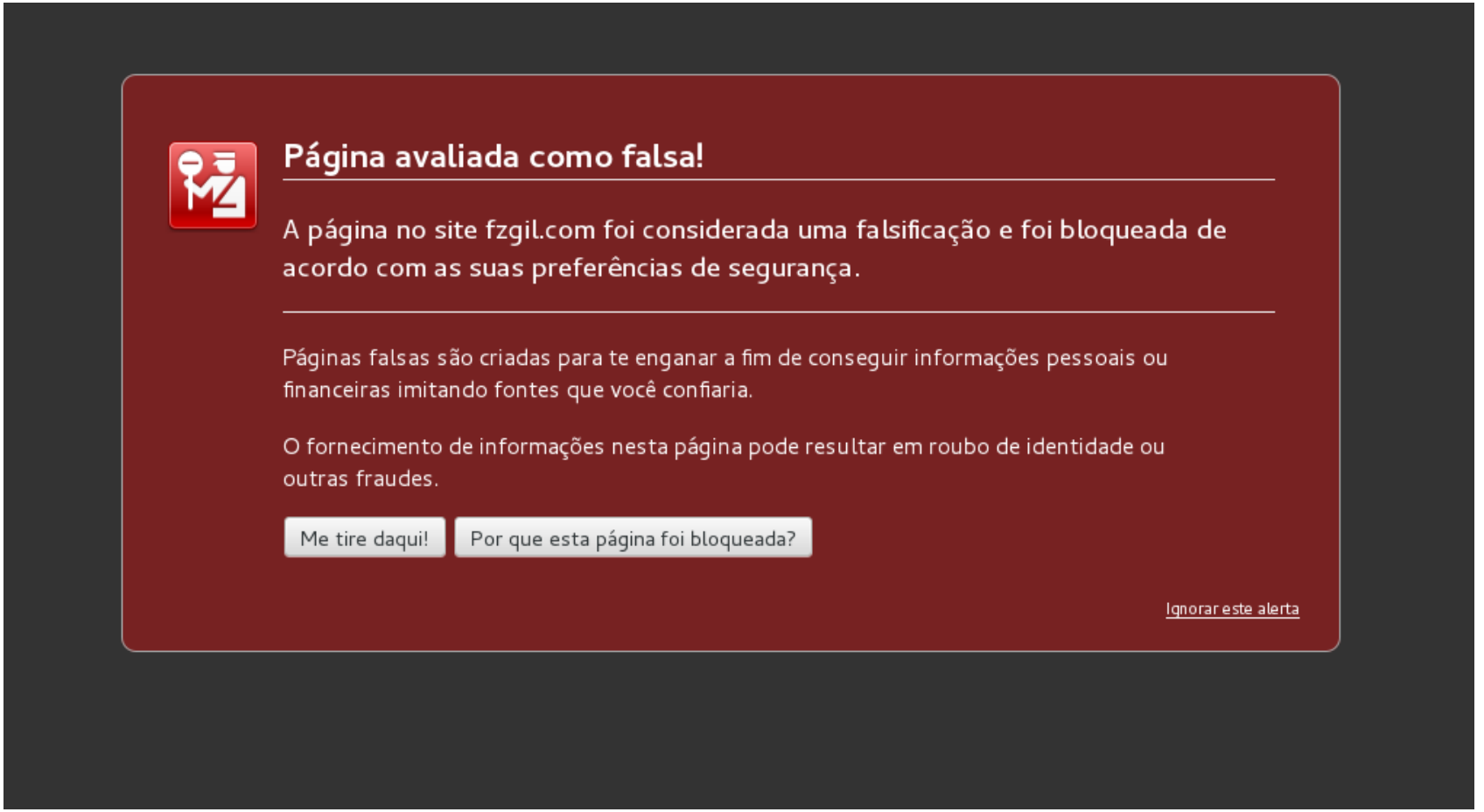


Evite ser Fisgado

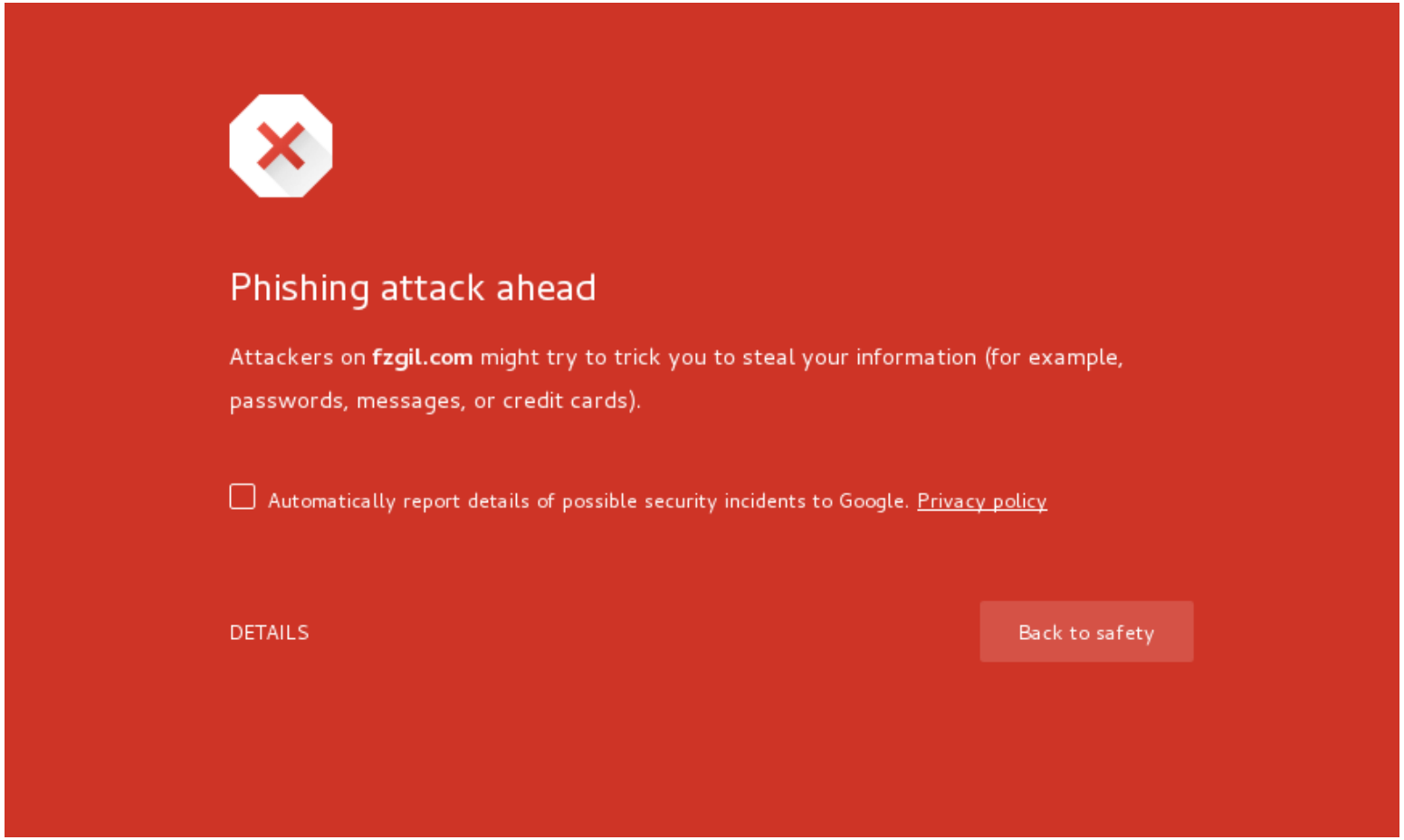
- Fazer backup e certificar que estão íntegros.
  - Proteção contra ataques de ransomware.



Não ignore os alertas



Não ignore os alertas



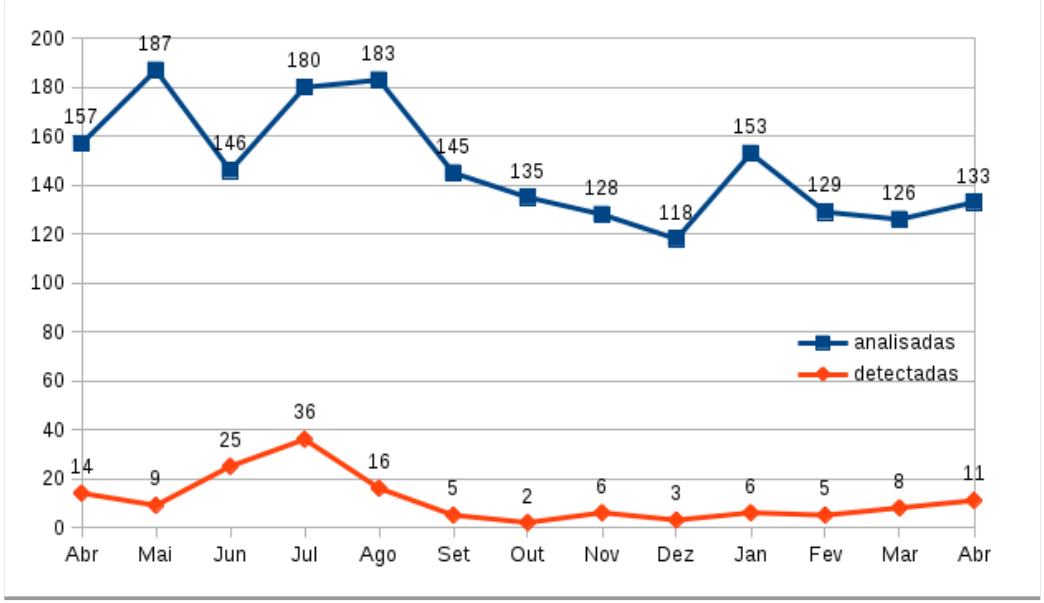
Catálogo de Fraudes do CAIS/RNP

Fonte: http://www.rnp.br/serviços/seguranca/catalogo-fraudes

phishing@cais.rnp.br

Catálogo de URLs Maliciosas

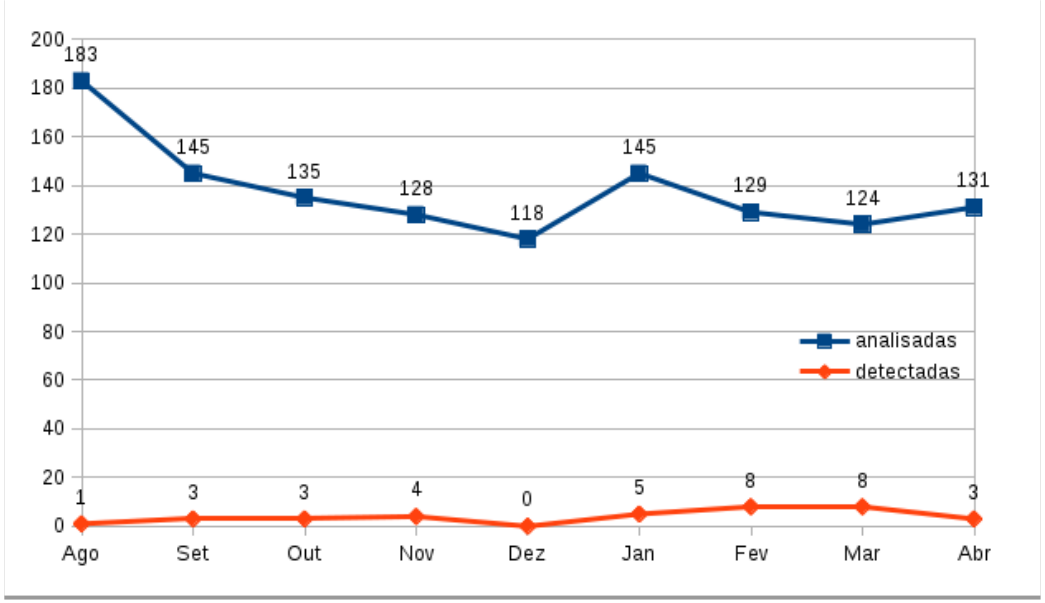
- Google Safe Browsing



URLs testadas x URLs detectadas

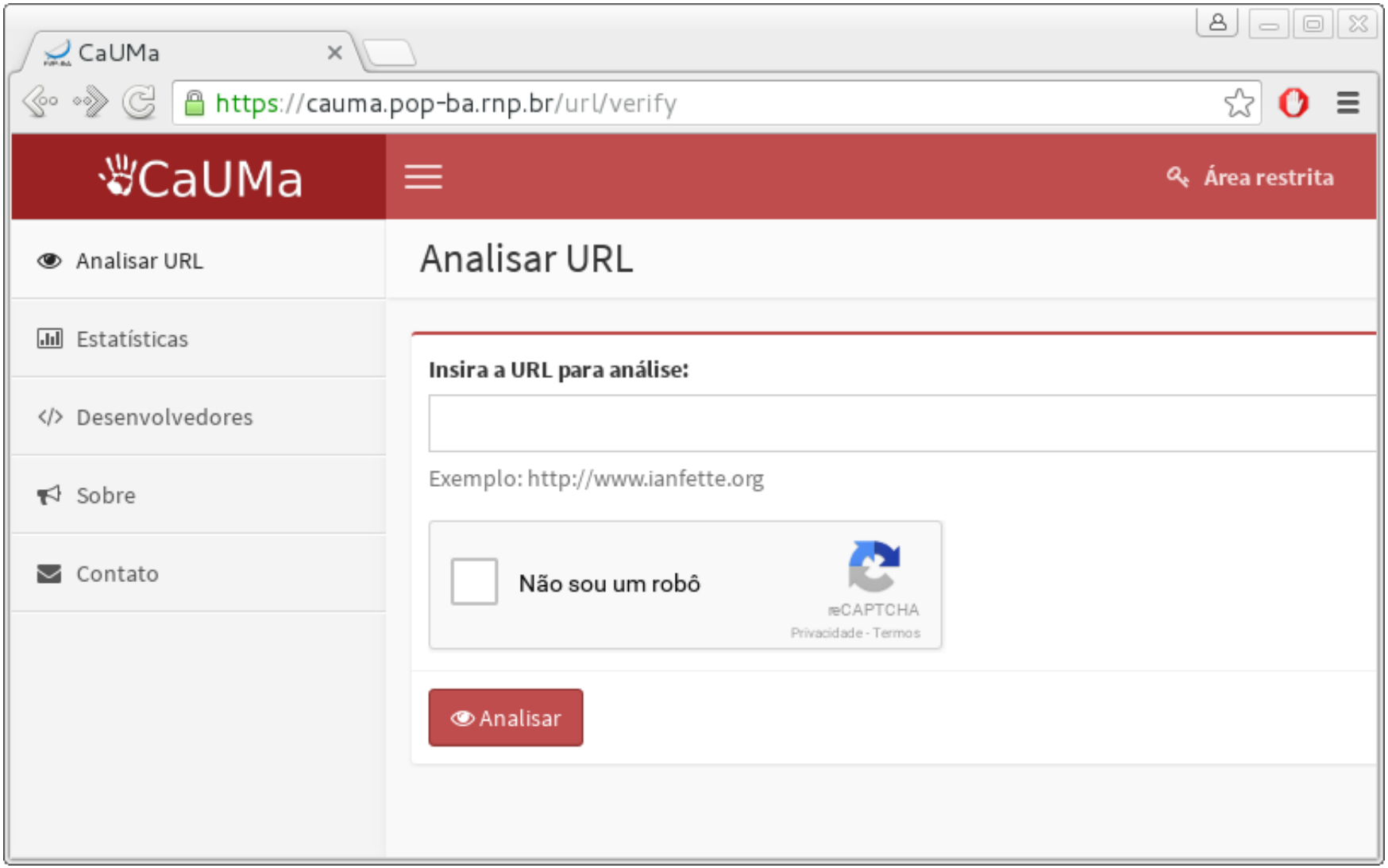
Catálogo de URLs Maliciosas

- Phishtank



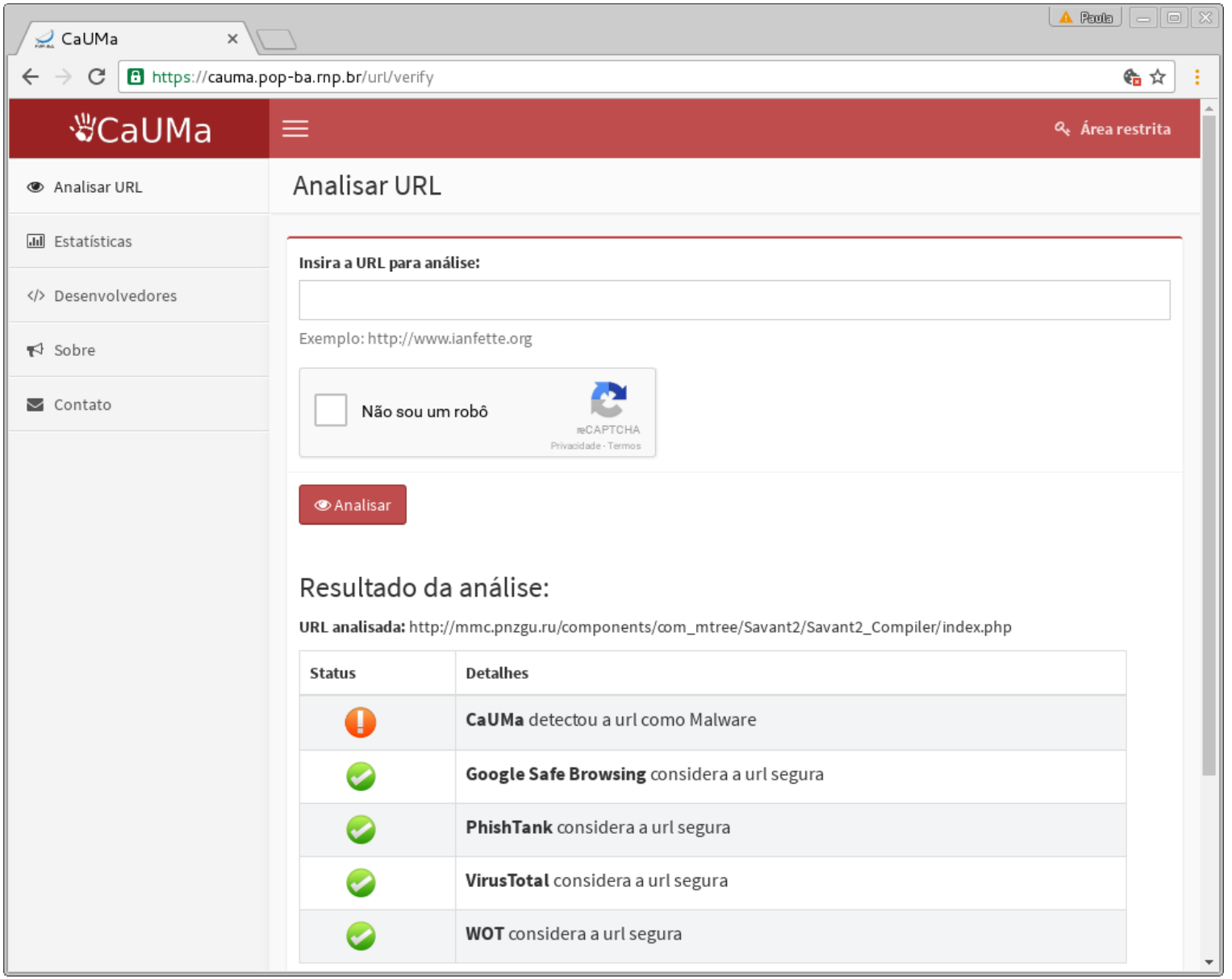
URLs testadas x URLs detectadas

Catálogo de URLs Maliciosas



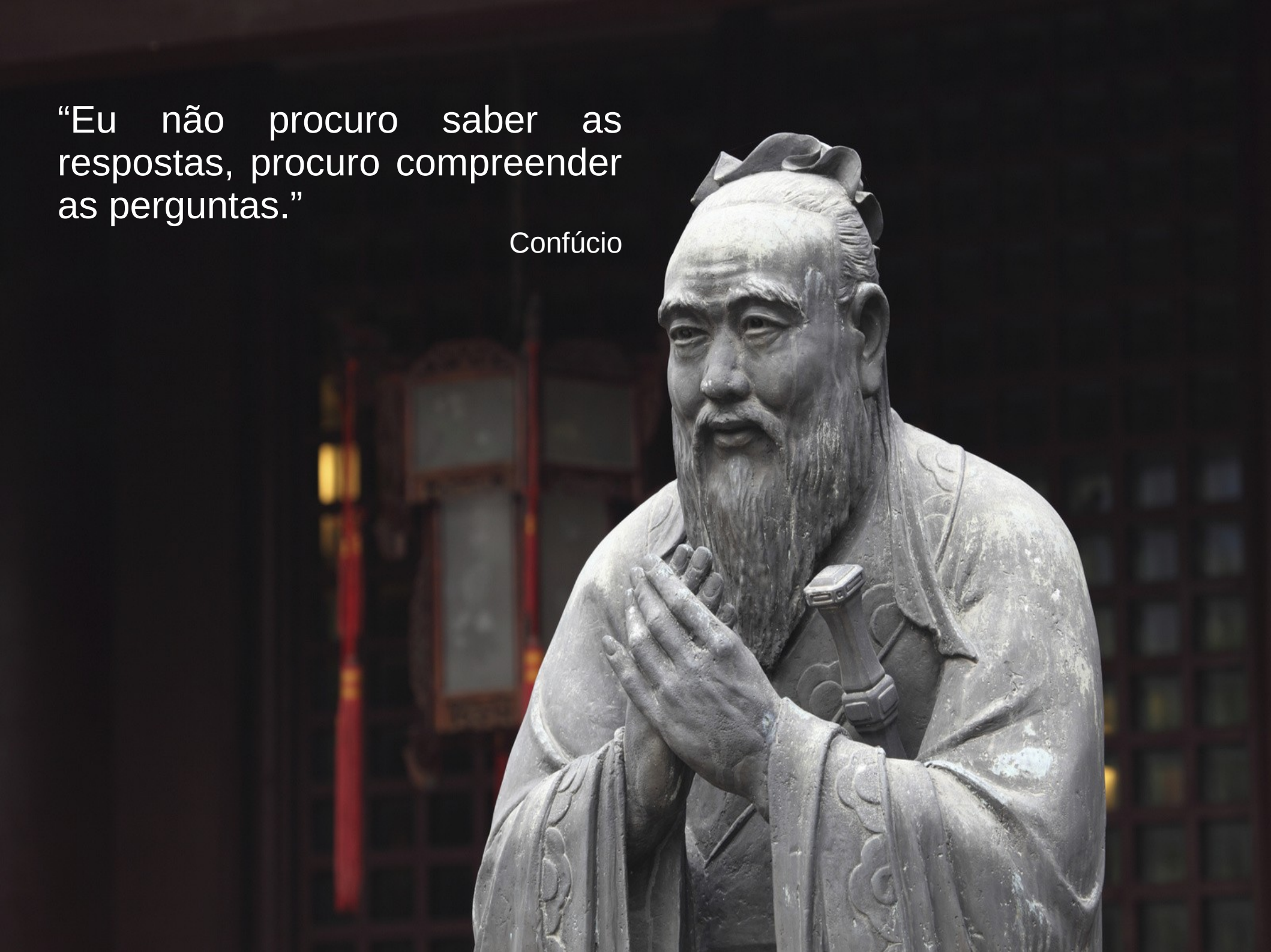
Fonte: https://cauma.pop-ba.rnp.br/

Catálogo de URLs Maliciosas



O que fazer após ser fisgado

- Entrar em contato com a instituição verdadeira relacionada à fraude.
- Reportar para:
  - mail-abuse@cert.br: enviar informações do ocorrido e cópia do e-mail fraudulento.
  - phishing@cais.rnp.br: enviar cópia do e-mail fraudulento.
- Trocar as credencias fornecidas.


“Eu não procuro saber as respostas, procuro compreender as perguntas.”
Confúcio