

Outubro é o Mês de Segurança
no Brasil e na América Latina



FRAUDES NA INTERNET

Não seja vítima...

...nem vilão

VIII Encontro de Segurança em Informática

03 de outubro de 2018



Yuri Alexandro

**Analista de Sistemas
(UNEB)**

Bolsista/Estagiário/Técnico/Analista de TIC desde 2001

Analista de SegInfo desde 2009

Pós-Graduado em Gestão de Segurança da Informação

Trabalhou em equipes do IFBA, TJBA, UNEB e UFBA

**Colaborador do Centro de Atendimento a Incidentes de
Segurança – CAIS
(RNP)**





**Precisamos ter cuidado para não causar prejuízo
para nós mesmos e para outros.**

...

Phishing

**Cavalos de
tróia**

***Spear
phishing***

**Fraudes
financeiras**

BIOS

Spyware

Notícias Falsas

**Varredura de
portas**

APTs

Defacement

SPAM

**Negação de
serviço**

**Engenharia
Social**

**Direitos
autorais**

Sexting

**Roubo de
dados**

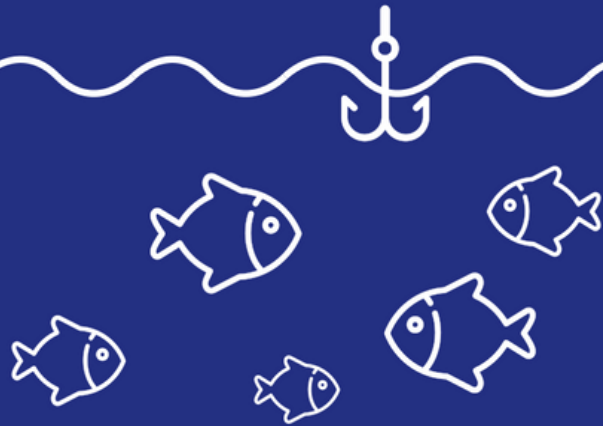
Botnets

Adware

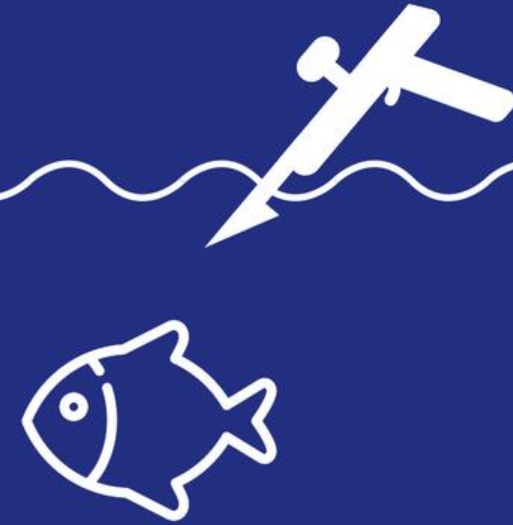
SMShing

Spear phishing

Spear phishing

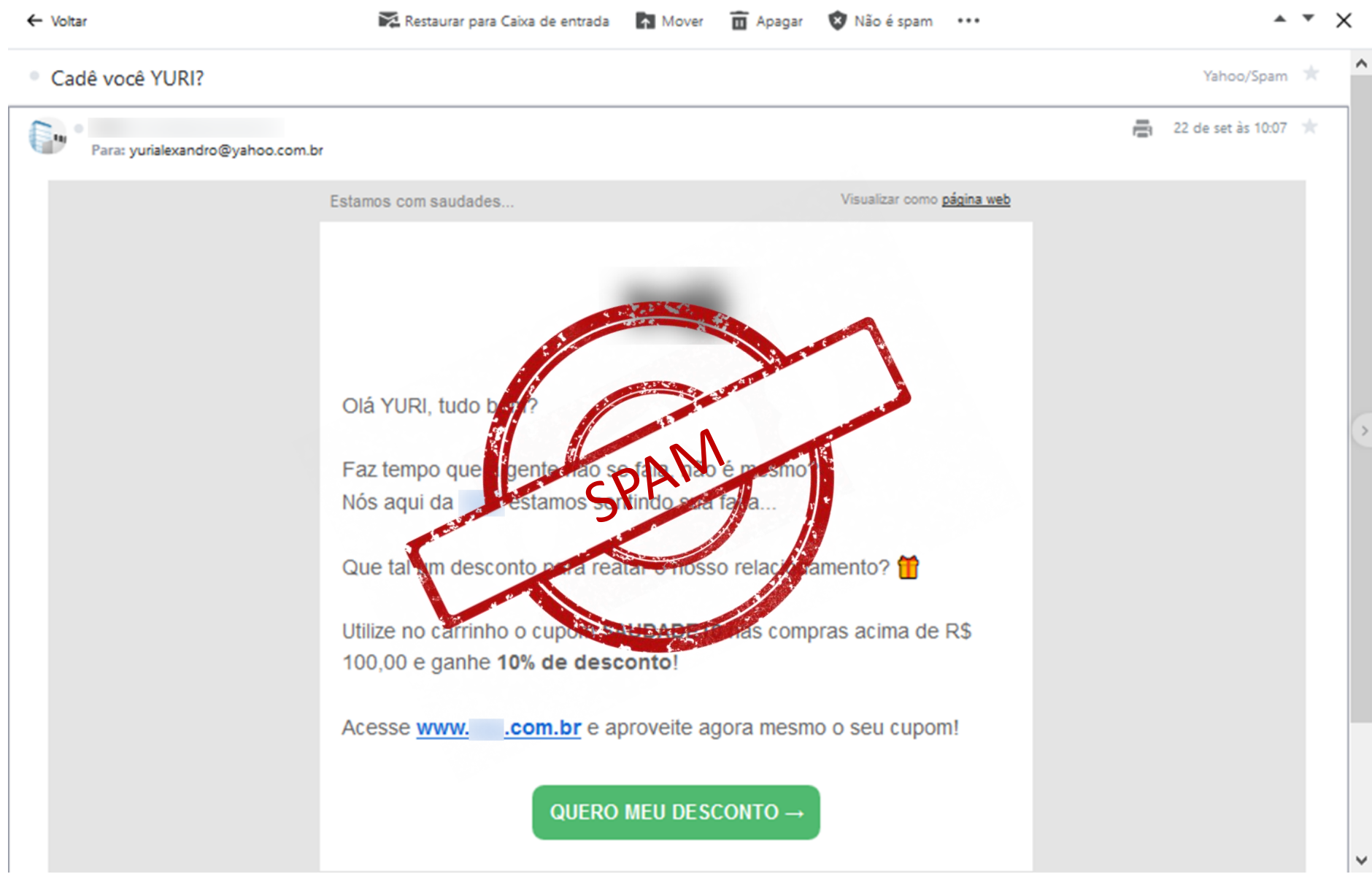


Phishing

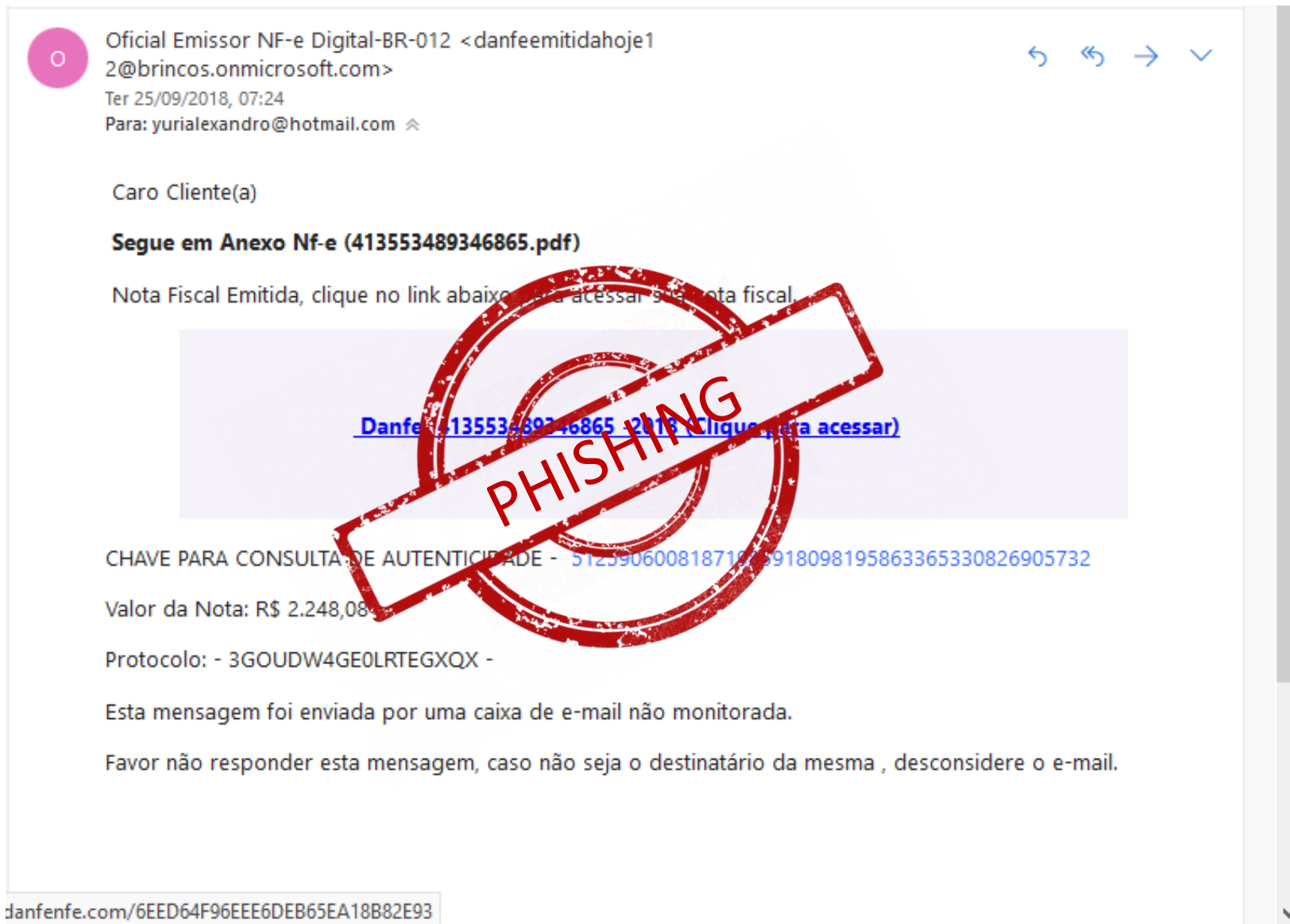


Spear Phishing

Spear phishing



Spear phishing



Spear phishing

IMAGEM DO CATÁLOGO DE FRAUDES CAIS/RNP
WWW.RNP.BR/CAIS/

CARO ufba.br USER,

Gostaríamos de informar que estamos actualmente a realizar a manutenção programada e melhorar o nosso serviço de webmail, e, como resultado, este vírus foi detectado em pastas HTK4S da sua conta e sua conta deve ser atualizado com a nova F Anti-virus/Anti - HTK4S de spam-Secure 2013 versão para evitar danos aos arquivos importantes. Preencher as colunas abaixo e enviar de volta ou a sua conta de e-mail será suspenso temporariamente de nossos serviços.

usuário:

password:

Data de Nascimento:

Ano-mail / criação da conta:

Se não o fizer dentro de 24 horas a sua conta será considerado não estiver em uso e ele será desativado completamente do nosso banco de dados webmail

Suporte ufba.br.

ufba.br Webmail EQUIPE

© Copyrights Reservados 2013

SPEAR PHISHING

Spear phishing

PREJUÍZOS

Uso da conta de e-mail para envio de novos *phishings*.

Causar interrupção do serviço de e-mail da instituição.

Permitir acesso do atacante a sistemas corporativos.

Atacante usa a conta para se passar pelo usuário e enganar outras pessoas.



Spear phishing

COMO EVITAR

DESCONFIE SEMPRE de e-mails suspeitos.
(quem mandou, gramática ruim, confirmação de senha, promessas fáceis, etc.)

EM HIPÓTESE ALGUMA abra anexos.

NUNCA clique em links.

CHEQUE informações sempre que necessário.



Catálogo de FRAUDES da RNP

O Catálogo de Fraudes da RNP é um repositório de fraudes eletrônicas que auxilia na identificação e ajuda na proteção contra golpes na Internet.

Com tantas novas fraudes a cada dia, é importante saber identificar as mensagens maliciosas recebidas por e-mail. Elas podem infectar seu computador com vírus, roubar informações pessoais e causar uma série de problemas.

O Brasil é um dos países com maiores índices de ataques de phishing. Cerca de 20% dos usuários brasileiros foram afetados no primeiro trimestre de 2018.

Acesse: catalogodefraudes.rnp.br

CAIS - Centro de Atendimento a Incidentes de Segurança
cais@cais.rnp.br

RNP

ENSI

MÊS de SEGURANÇA

11

Spear phishing

phishing@cais.rnp.br

Catálogo de FRAUDES da RNP

O Brasil é um dos países com maiores índices de ataques de phishing. Cerca de 20% dos usuários brasileiros foram afetados no primeiro trimestre de 2018.

Com tantas novas fraudes a cada dia, é importante saber identificar as mensagens maliciosas recebidas por e-mail. Elas podem infectar seu computador com vírus, roubar informações pessoais e causar uma série de problemas.

O Catálogo de Fraudes da RNP é um repositório de fraudes eletrônicas que auxilia na identificação e ajuda na proteção contra golpes na Internet.

Acesse: catalogodefraudes.rnp.br

CAIS - Centro de Atendimento a Incidentes de Segurança
cais@cais.rnp.br

RNP

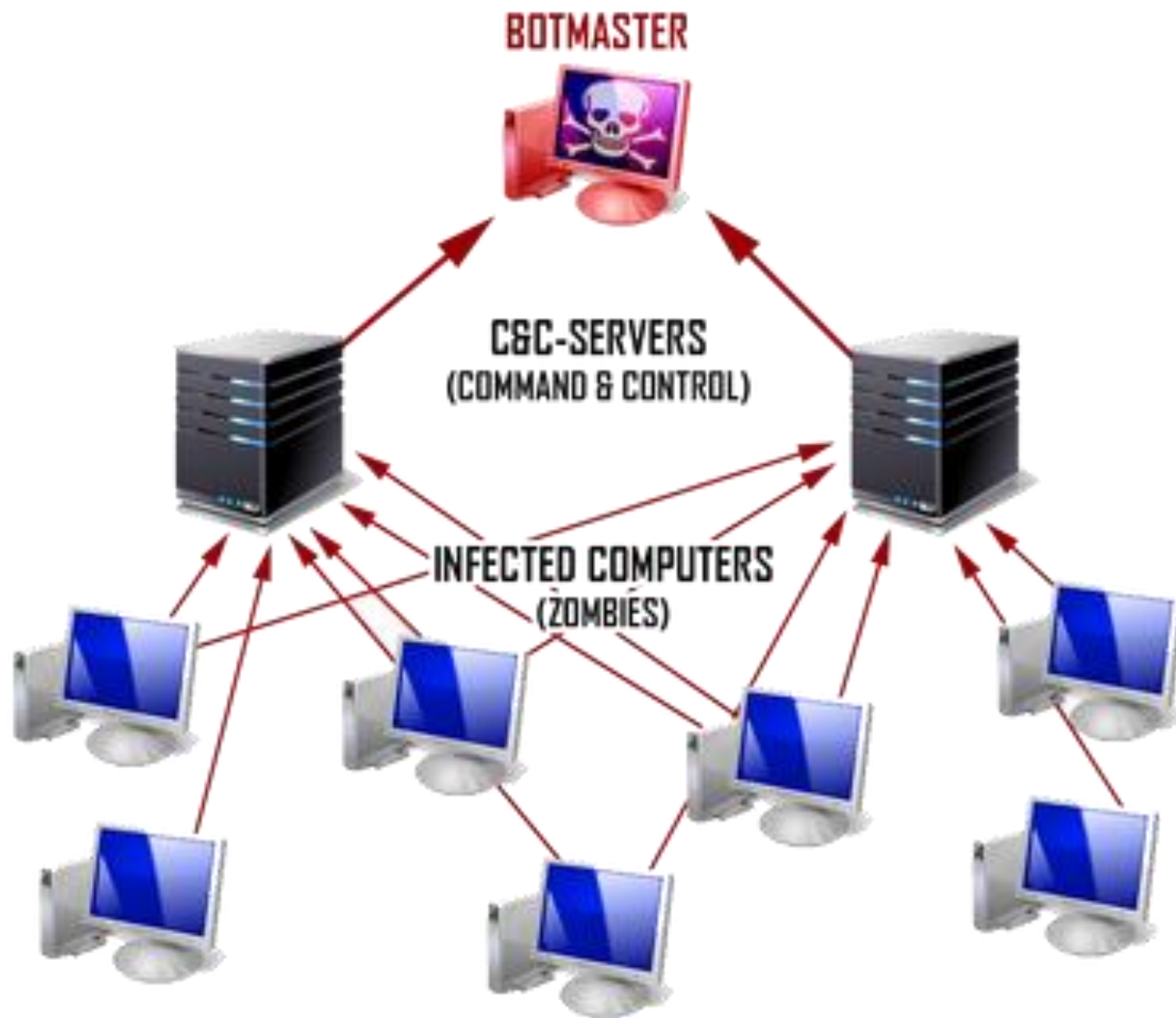
ENSI

MÊS de SEGURANÇA

CAIS 12 RNP

Botnets

Botnets

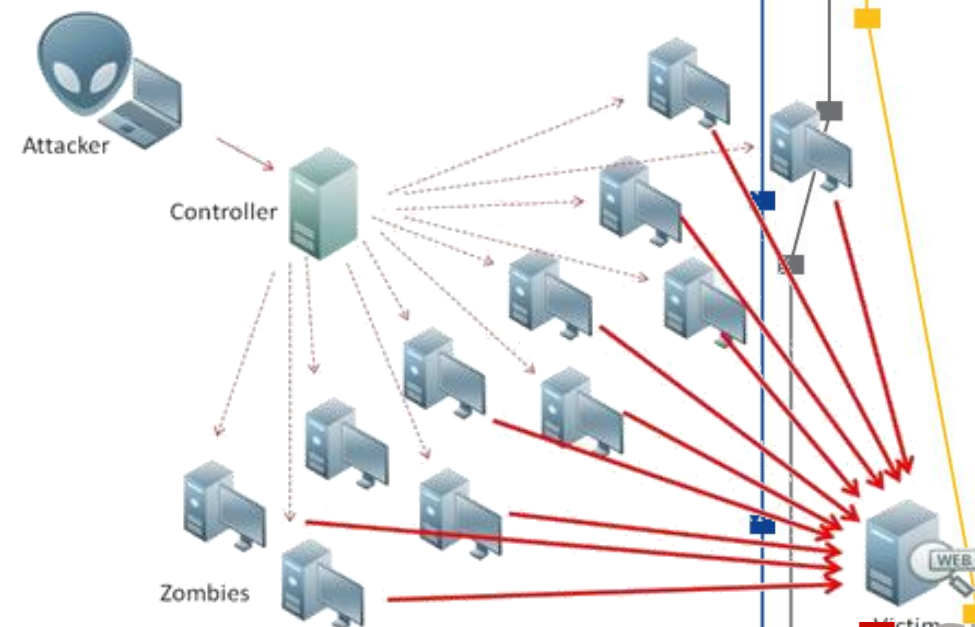
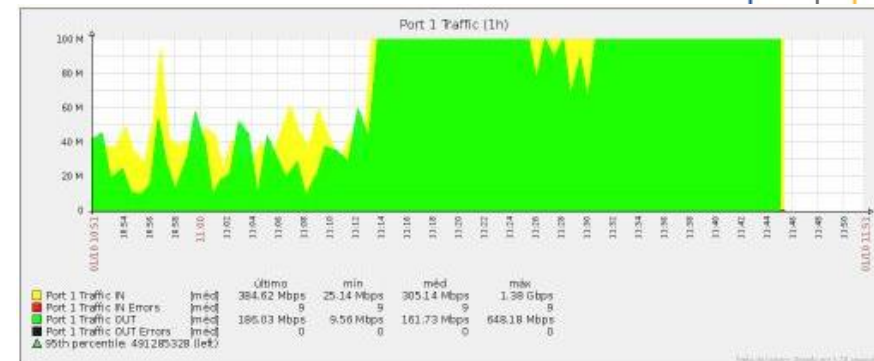


PREJUÍZOS

Acesso não-autorizado à arquivos e informações pessoais e confidenciais.

Uso de recursos do computador para fins não autorizados ou ilícitos (ex. cryptojacking).

Uso do computador ou dispositivo em incidentes de segurança da informação.



COMO EVITAR

**DESCONFIE SEMPRE, EM HIPÓTESE ALGUMA,
NUNCA, CHEQUE...**

TENHA CUIDADO ao baixar arquivos, não abra e-mails
suspeitos.

NÃO CLIQUE em links recebidos de e-mails, nem acesse
sites suspeitos.

USE E ABUSE de softwares antivírus eficientes.

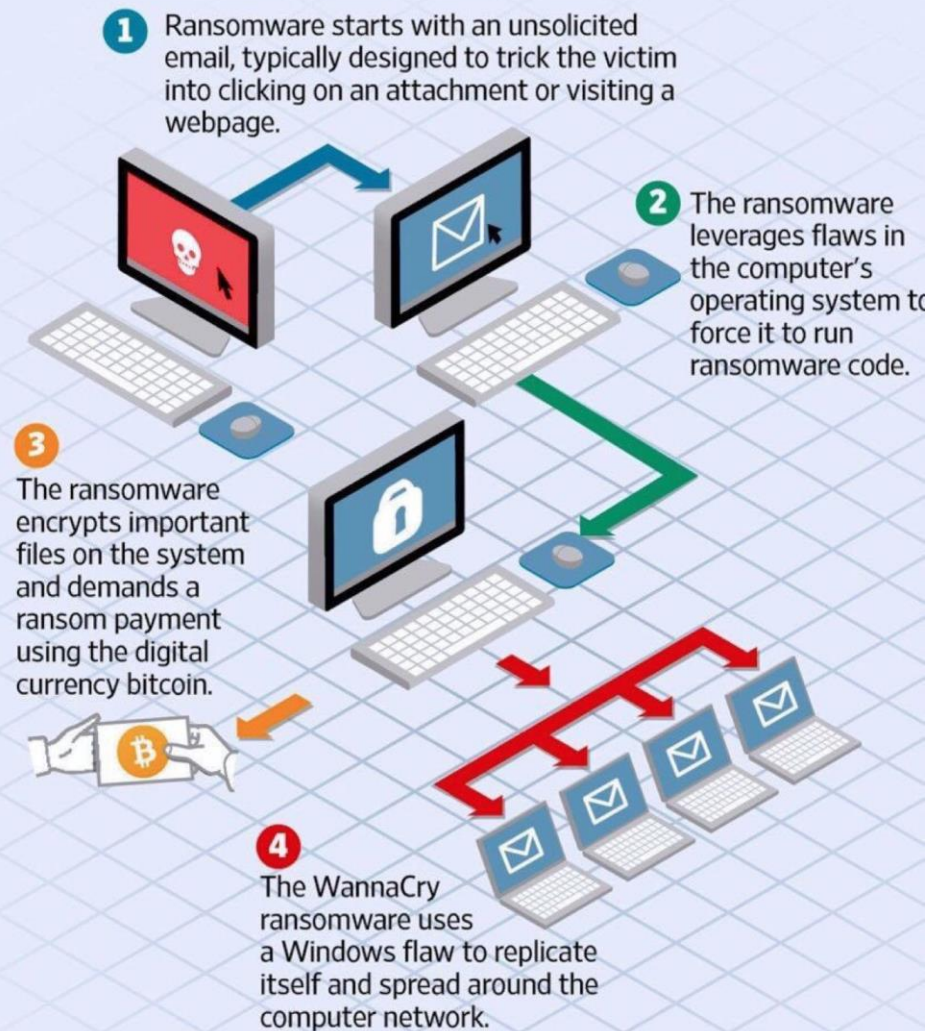
ATUALIZE sempre seu computador ou dispositivo móvel.



Ransomwares



How Ransomware Works



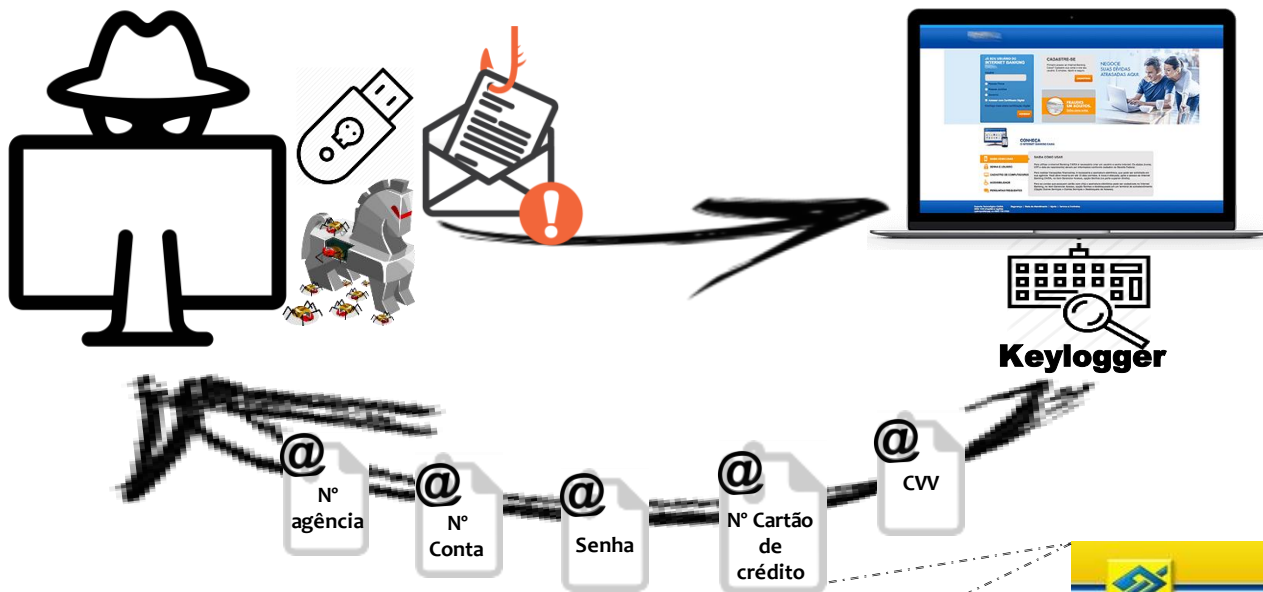
Source: staff reports

THE WALL STREET JOURNAL

Fraudes Financeiras

**De quantos modos seus
dados bancários podem
ser roubados?**

Fraudes financeiras



Instalação de malwares

Keylogger

Alteração do arquivo de
resolução de nomes (hosts)

```
hosts - Bloco de notas
Arquivo Editar Formatar Exibir Ajuda
Copyright (c) 1993-2009 Microsoft Corp.

This is a sample HOSTS file used by Microsoft TCP/IP for Windows.

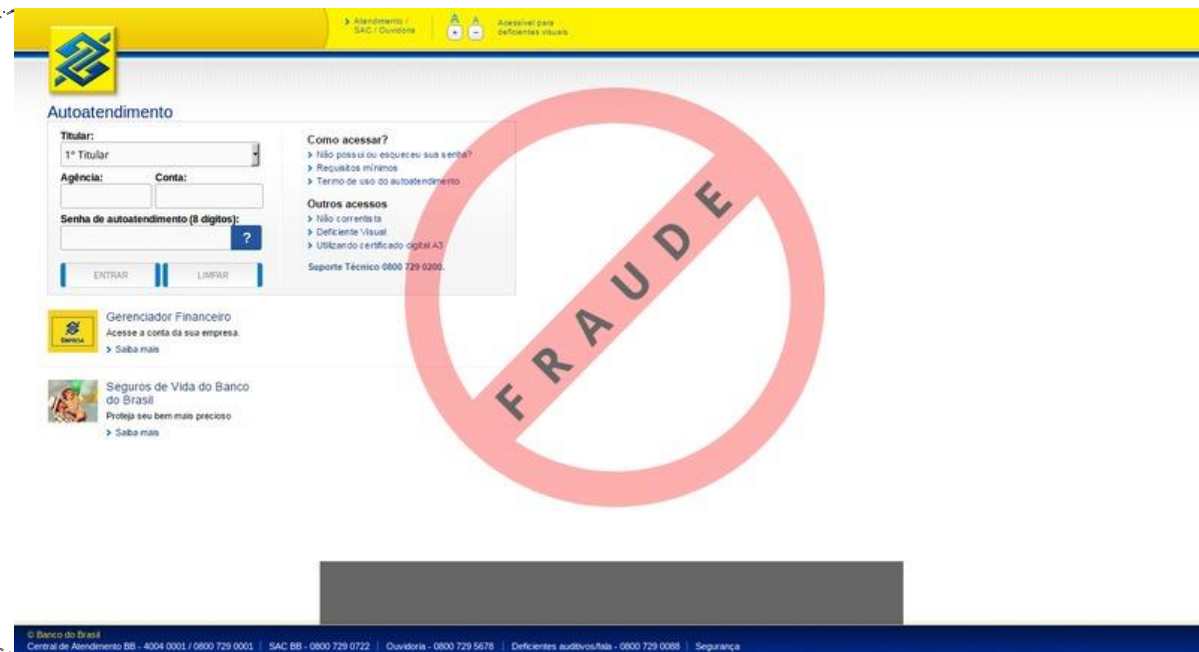
This file contains the mappings of IP addresses to host names. Each
entry should be kept on an individual line. The IP address should
be placed in the first column followed by the corresponding host name.
The IP address and the host name should be separated by at least one
space.

Additionally, comments (such as these) may be inserted on individual
lines or following the machine name denoted by a '#' symbol.

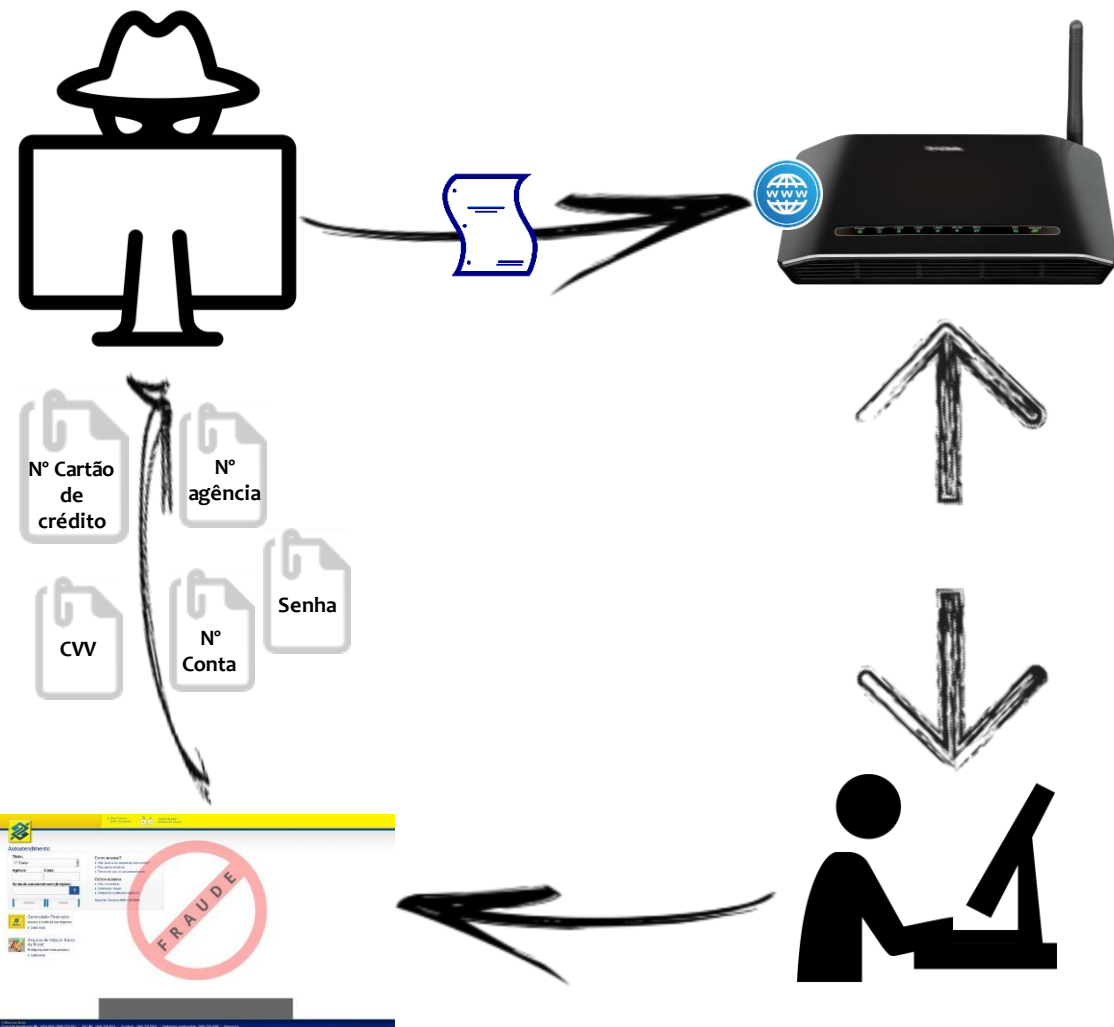
For example:
#102.54.94.97 rhino.acme.com      # source server
#38.25.63.10  x.acme.com         # x client host

# localhost name resolution is handled within DNS itself.
#127.0.0.1 localhost
#::1 localhost

127.0.0.1 www.google.com.br
198.106.228.156 citibank.com.br
198.106.228.156 citibank.com
198.106.228.156 infoseg.gov.br
198.106.228.156 real.com.br
198.106.228.156 bancoreal.com.br
198.106.228.156 unibanco.com
198.106.228.156 unibanco.com.br
198.106.228.156 ww.bb.com.br
```



Fraudes financeiras



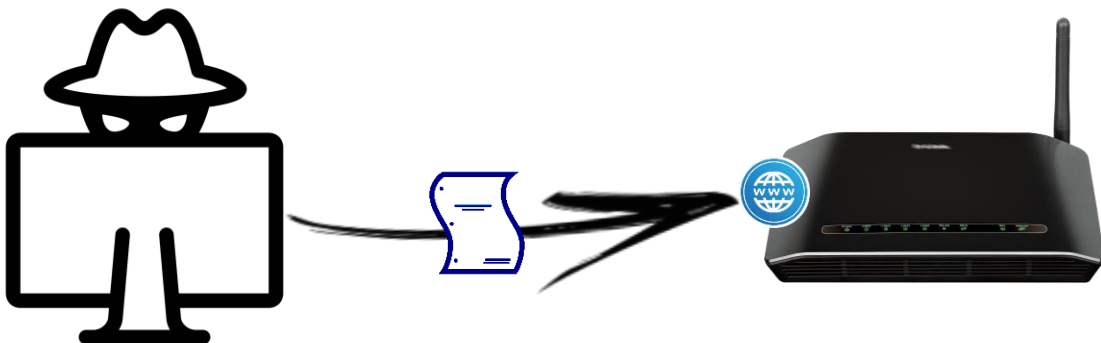
Comprometimento de modems/roteadores ADSL

Alteração do servidor de resolução de nomes (DNS)

Vulnerabilidade: modem está configurado com senha padrão ou de fácil descoberta

Computador não é comprometido, mas a conexão é maliciosa

Fraudes financeiras



Comprometimento dos modems ADSL

Alteração do servidor de resolução de nomes (DNS)

Achieving Together

Status

Basic

- ADSL Mode
- WAN Setting
- LAN Setting
- DHCP
- NAT
- IP Route
- ATM Traffic

Advanced

Tools

DHCP

DHCP Settings

DHCP	Server
Client IP Pool Starting Address	192.168.1.100
Size of Client IP Pool	135
Primary DNS Server	66.110.243
Secondary DNS Server	8.8.8.8
Remote DHCP Server	N/A
DHCP Lease Time	0 Days 0 Hours 15 Min
WAN Primary DNS Server	66.110.243
WAN Secondary DNS Server	8.8.8.8

DHCP Table

Host Name	IP Address	MAC Address
TL-WR340G	192.168.1.100	00:25:86:DB:FC:B5

Submit

Autoatendimento

Título:

1º Titular

Agência:

Conta:

Senha de autoatendimento (8 dígitos):

ENTRAR

Como acessar?

- Não possui ou esqueceu sua senha?
- Requisitos mínimos
- Termo de uso do autoatendimento

Outros acessos

- Não é correntista
- Deficiente Visual
- Utilizando o certificado digital A3

Suporte Técnico 0800 729 0300

Gerenciador Financeiro

Acesse a conta da sua empresa.

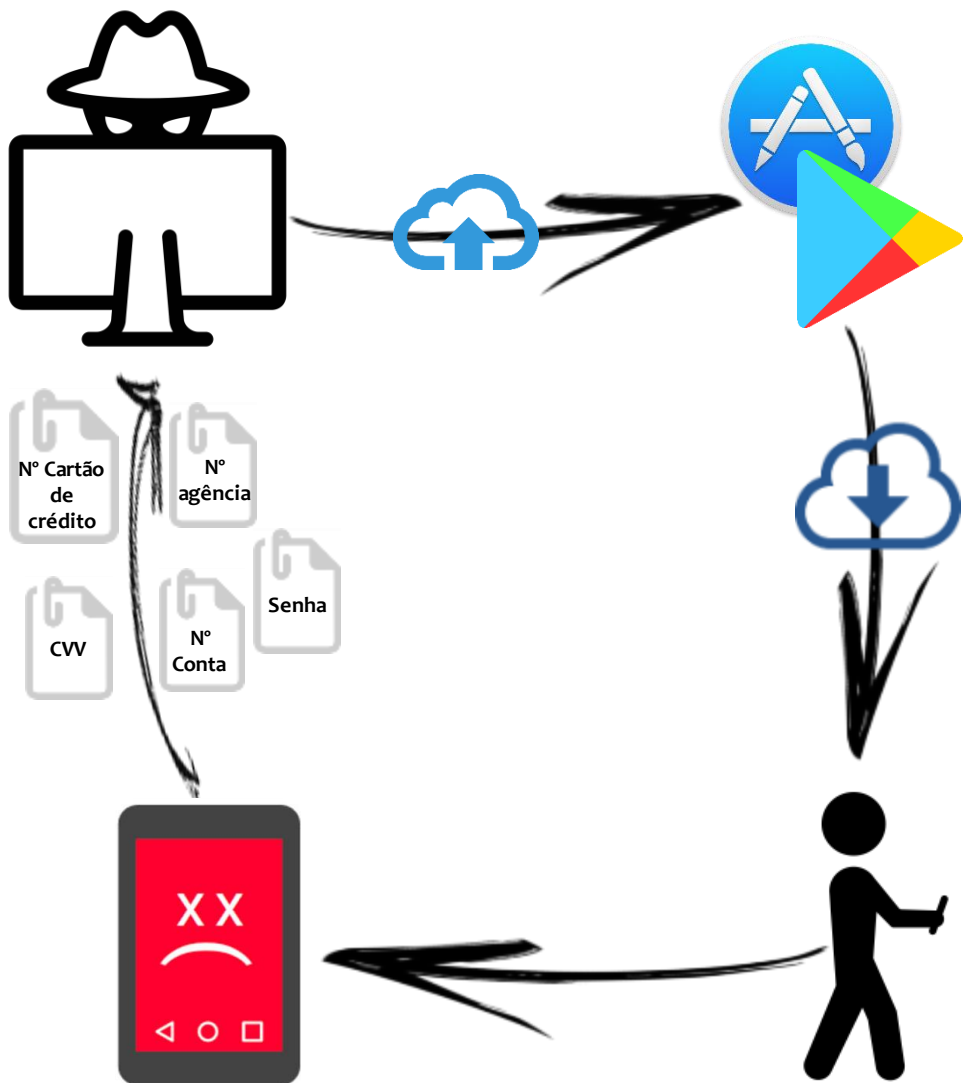
Seguros de Vida do Banco do Brasil

Proteja seu bem mais precioso

FRAUDE

© Banco do Brasil
Central de Atendimento BB - 4004 0001 / 0800 729 0001 | SAC BB - 0800 729 0722 | Ouvidoria - 0800 729 5678 | Deficientes auditivos/fisais - 0800 729 0308 | Segurança

Fraudes financeiras



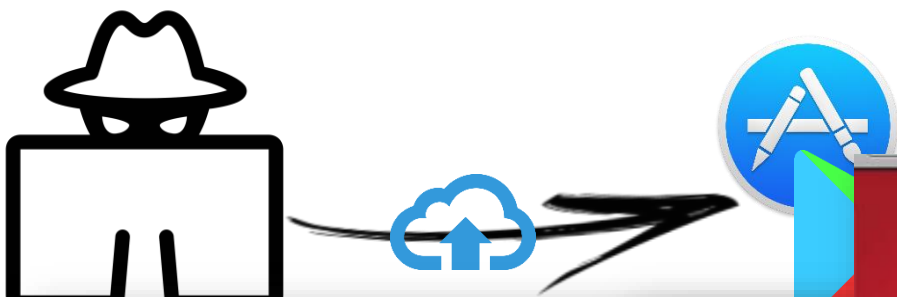
Apps falsos para tablets/celulares

Disponíveis nas lojas (AppStore ou GooglePlay)

Usuário instala aplicativo malicioso

Apps podem ser porta de entrada para instalação de mais malwares

Fraudes financeiras



Apps falsos para tablets/celulares



Descrição

Com o aplicativo do [redacted] você tem acesso a Conta Pessoal (Pe) para realizar lançamentos futuros, pagamentos (inclusive com a câmera), realizar transferências de pagamentos, pagamento eletrônico de salários, etc. Além disso, você pode utilizar o [redacted] para realizar transações pela internet da Central de Atendimento, etc.

Para acesso a sua Conta Pessoal, é necessário a senha de 8 dígitos, a mesma financeira, será exigida a senha de 6 dígitos.

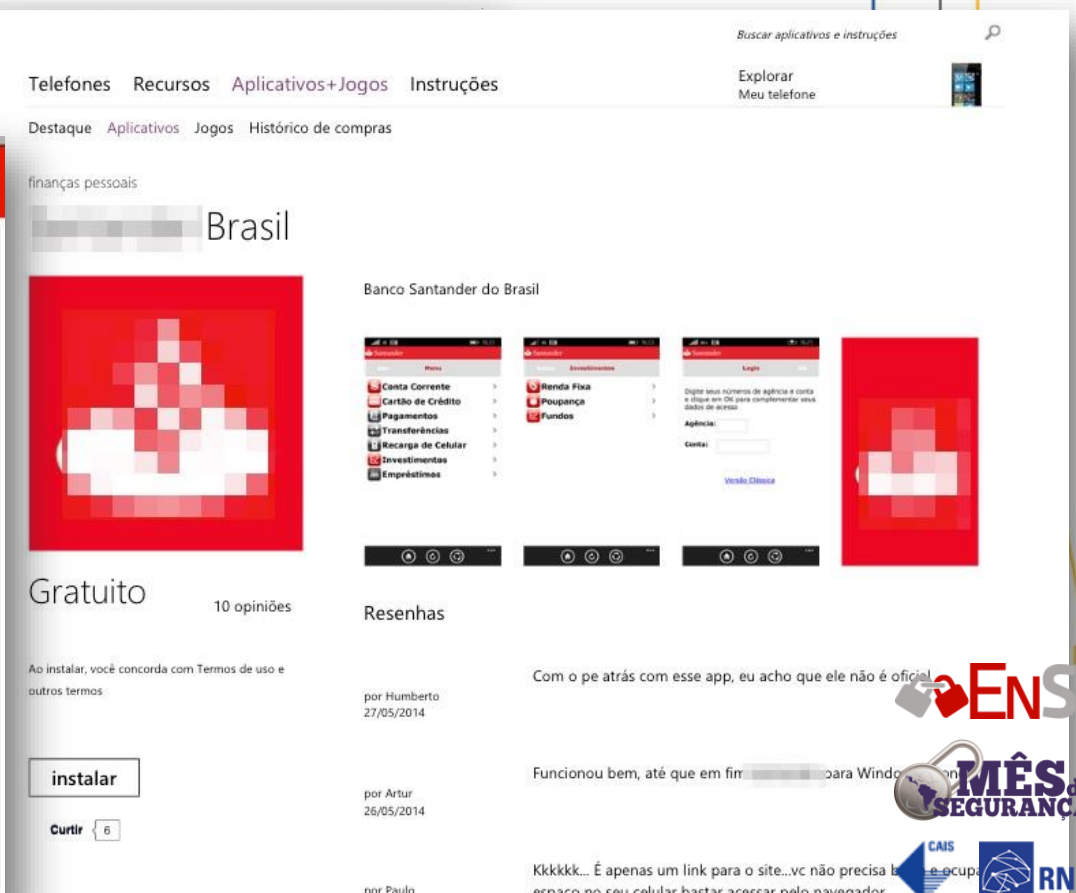
Para acesso a Conta de sua Empresa (Gerenciador Financeiro, PJ), são necessárias a senha de 8 dígitos, as mesmas utilizadas no Gerenciador Financeiro pela



Descrição

Com a nova versão do aplicativo do [redacted] do cartão de crédito, você pode realizar transações financeiras. E você também pode realizar transações de financiamento.

Facilidade, rapidez



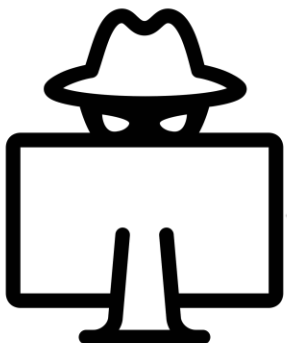
Fraudes financeiras



Apps falsos para tablets/celulares



Fraudes financeiras



Santander 03371 00129.63290 64000.000006 00125.201020 4 56140000017832

Beneficiário		CPF/CNPJ do Beneficiário		Assinatura	
Nome Completo		CPF/CNPJ do Beneficiário		Assinatura	
Valor do Boleto		Quantidade		Valor do Boleto	
R\$		R\$		R\$	
Instruções - Leia as Instruções do Beneficiário					
FRAUDE					
Pagador		CPF/CNPJ do Pagador		Assinatura	
Nome Completo		CPF/CNPJ do Pagador		Assinatura	
Valor do Boleto		Quantidade		Valor do Boleto	
R\$		R\$		R\$	
Autenticação Mecânica - Ficha de Compensação					

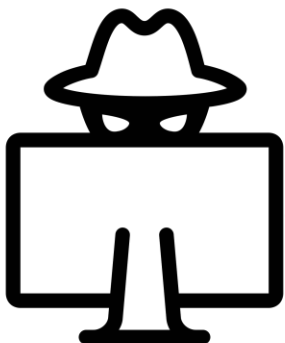
Boletoware

Sites falsos com promoções “imperdíveis”

Site gera um boleto com o valor que será “pago” ao atacante.

Boletos podem ser falsos ou verdadeiros.

Fraudes financeiras



Smart TV Samsung LED 50"
UN50FH5303GXZD Full HD 2 HDMI USB
120Hz

De R\$ 2.199,00
Por
R\$ **856,90** à vista

Boletoware falso

237 = Bradesco / 39 = HSBC
Logotipo do Bradesco e código do HSBC

Código que identifica o cliente no banco diferente do que está indicado no boleto

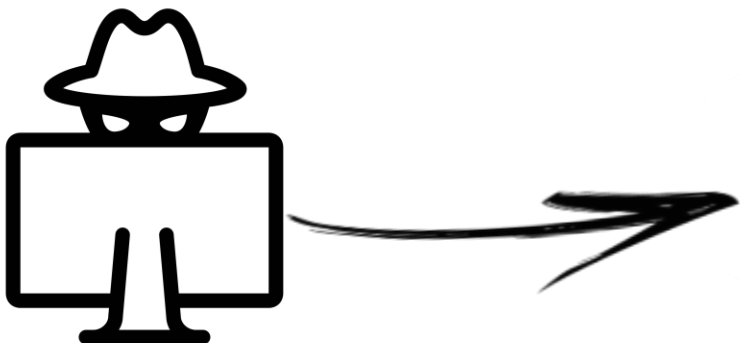
Obs: ignorar o dígito depois da agência.

Bradesco **237-2** **399** 30.82227 68406.0 **19691** 83006.33 0012 5 65160000022663

Local de pagamento				Pagável em qualquer Banco até o vencimento		Vencimento	
Cedente				Teste LTDA		30/03/2015	
Data do documento				Nº documento		Agência Cedente	
21/07/2015				0000272539		0543 05431218979	
Especie doc.				Aceite		Nosso número	
DS				21/07/2015		18222684060	
Uso do banco				Carteira		Valor Documento	
Especie				Quantidade		(n) Valor documento	
R\$				001		226.63	
Instruções (Texto de responsabilidade do cedente)						(c) Desconto / Abatimentos	
- Sr. Caixa, cobrar multa de 2% após o vencimento						(c) Outras deduções	
- Receber até 10 dias após o vencimento						(+) Mora / Multa	
- Em caso de dúvidas entre em contato conosco: ederson.dev@gmail.com						(+) Outros acréscimos	
Sacado						(n) Valor cobrado	
João Açução							
Um end. de teste - Bairro-teste							
Sobradinho - DF - CEP:73080190							
Sacador/Analista						Cód. baixa	
						Autenticação mecânica - Ficha de Compensação	

FRAUDE!

Fraudes financeiras



Smart TV Samsung LED 50"
UN50FH5303GXZD Full HD 2 HDMI USB
120Hz

De R\$ 2.199,00
Por
R\$ **856,90** à vista

Boletoware legítimo

Boleto

169.54.79.121/zn/produtos/Boleto/01/Boleto008.html

Search

Por favor, confira os campos abaixo antes de pagar o seu boleto

Após imprimir, compare as informações do boleto com as do modelo abaixo. Caso exista alguma divergência não pague o boleto e entre em contato com nosso atendimento.

modelo boleto

Confira a identificação do banco

BANCO DO BRASIL

000-0

Confira os algarismos do boleto

00190.00009 02597.731

00000000.000000 0 0000000000000000

Local de pagamento

Nome do banco

Vencimento

00/00/0000

Beneficiário

Agência/Código do Beneficiário

0000-0/00000-0

Data Documento

00/00/0000

Número do Documento

000000000

Espécie Doc.

0

Data Processamento

00/00/0000

Nosso Número

00000000000000000000

Confira o nome do beneficiário e o CNPJ

BANCO DO BRASIL

001-9

00190.00009 02597.731054 93249.111183 1 65530000161696

Beneficiário			Agência/Código do Beneficiário		Vencimento	
			3070-8/15300-1		16/09/2015	
Pagador			Número do Documento		Nosso Número	
Cliente			593249111		25977310593249111	
Especie	Quantidade	(x) Valor	(-) Descontos / Abatimentos		(=) Valor Documento	
R\$					1.616,96	
Demonstrativo:			(+) Outros Acréscimos		(=) Valor Cobrado	

BANCO DO BRASIL

001-9

00190.00009 02597.731054 93249.111183 1 65530000161696

Local de Pagamento			Vencimento		
Banco do Brasil S.A			16/09/2015		
Pagável preferencialmente em qualquer Agência Banco do Brasil					
Beneficiário			Agência/Código do Beneficiário		
			3070-8/15300-1		
Data Documento	Número do Documento	Espécie Doc.	Acelte	Data Processamento	Nosso Número

ENSI

MÊS de SEGURANÇA

CAIS

RNP

COMO EVITAR

**DESCONFIE SEMPRE, EM HIPÓTESE ALGUMA,
NUNCA, CHEQUE...**

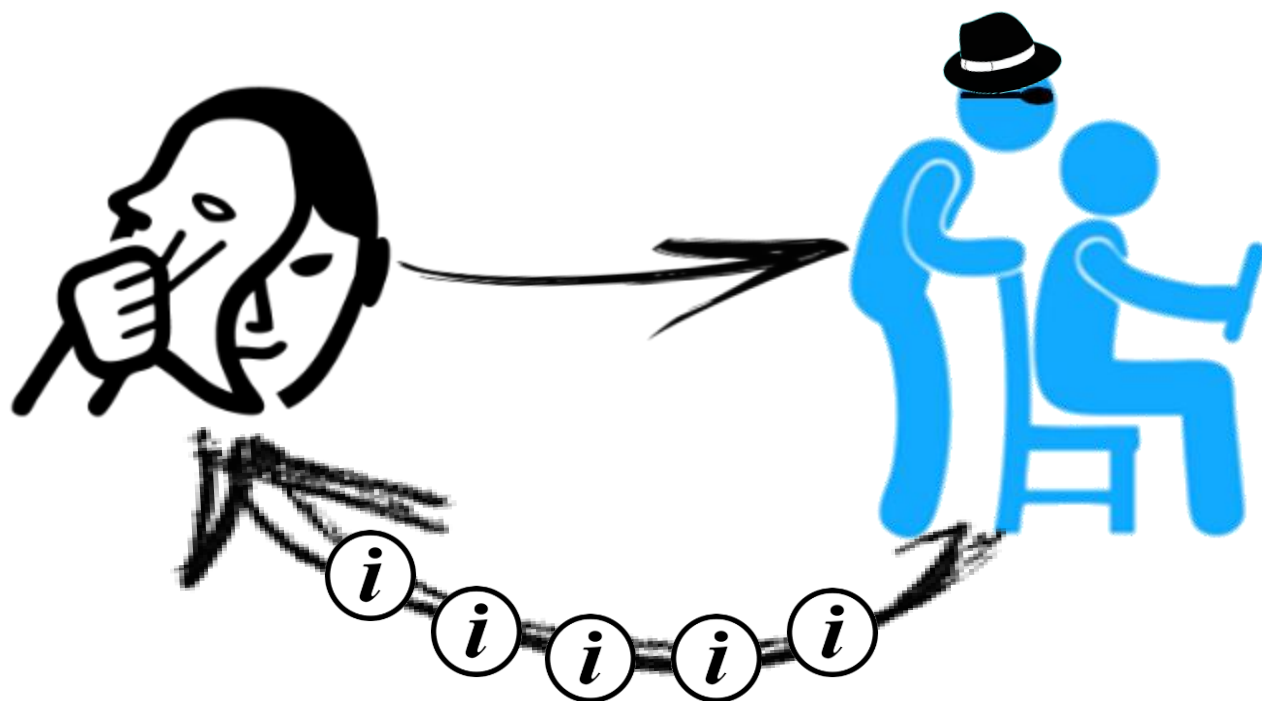
TENHA CUIDADO ao baixar apps, leia com atenção
os comentários e não use se ver algo suspeito.

SEJA RETICENTE ao receber promessas de
promoções mirabolantes.

TROQUE A SENHA PADRÃO do seu roteador wifi,
e escolha senhas fortes.



Engenharia Social



“A arte de enganar”

Pessoas mal-intencionadas se fazem passar por outras ou fingem possuir cargos que não tem.

Usuário é levado a acreditar na história contada.

Objetivo de obter informações confidenciais e sigilosas.





“A arte de enganar”





VÍDEO

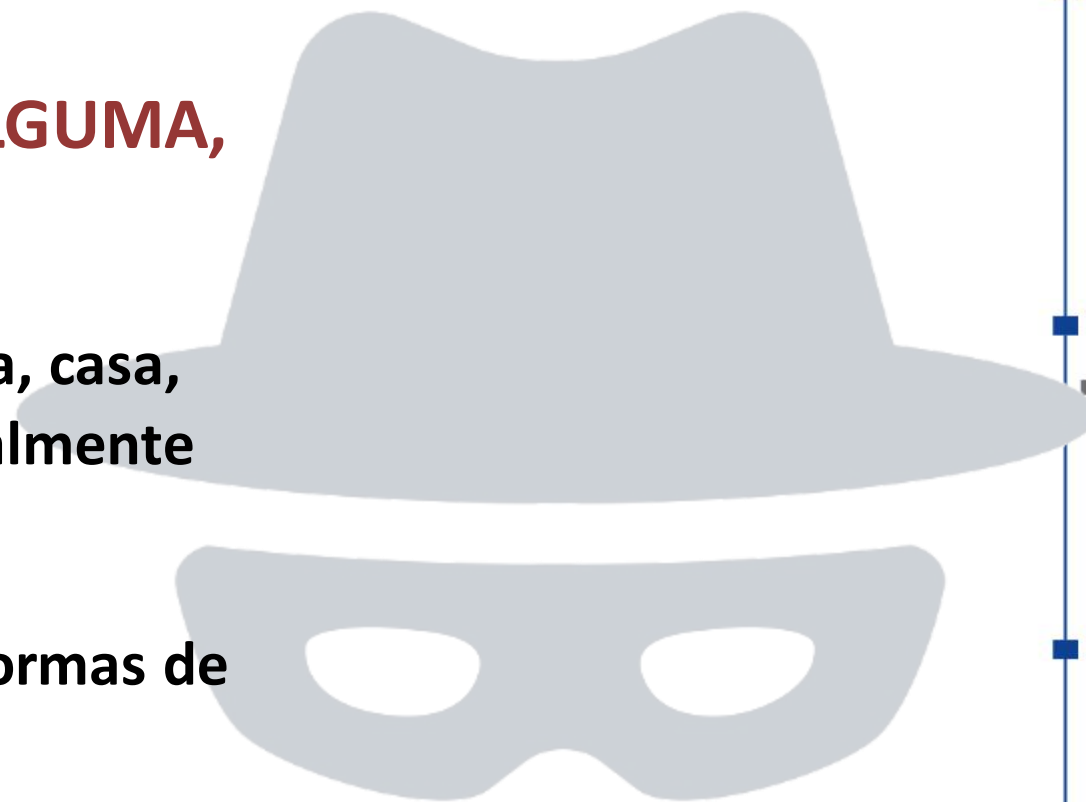
<https://youtu.be/QskBef2mGnU>

COMO EVITAR

**DESCONFIE SEMPRE, EM HIPÓTESE ALGUMA,
NUNCA, CHEQUE...**

NÃO REPASSE informações de sua rotina, casa,
local de trabalho sem saber para quem realmente
está falando.

SIGA IRRESTRITAMENTE as políticas e normas de
segurança da informação.





VÍDEO

<https://youtu.be/Wal6Z6MEMew>



RNP



sd@rnp.br



0800 722 0216



(61) 9 9960 5971



1916*800



cais@cais.rnp.br



MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
**CIÊNCIA, TECNOLOGIA,
INOVAÇÕES E COMUNICAÇÕES**

