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

RNP

MINISTÉRIO DA DEFESA
MINISTÉRIO DA CULTURA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES

BRASIL GOVERNO FEDERAL

ENSI

CERT Bahia

PoP BA
Ponto de Presença da RNP na Bahia

RNP

CAIS

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

Fraudes financeiras

Spear phishing

BIOS

Notícias Falsas

Varredura de portas

Spyware

APTs

Defacement

SPAM

Negação de serviço

Engenharia Social

Direitos autorais

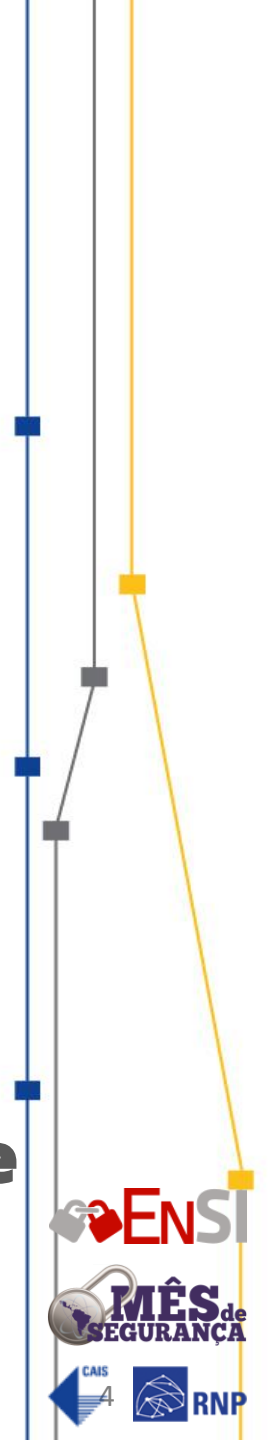
Adware

Botnets

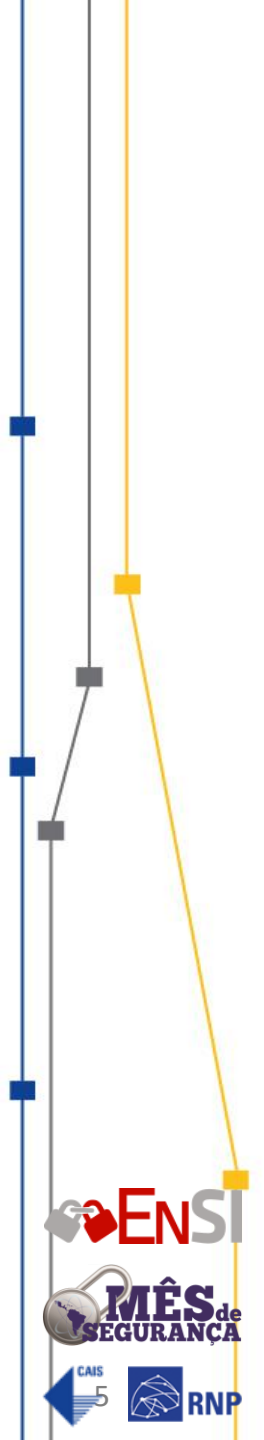
Sexting

Roubo de dados

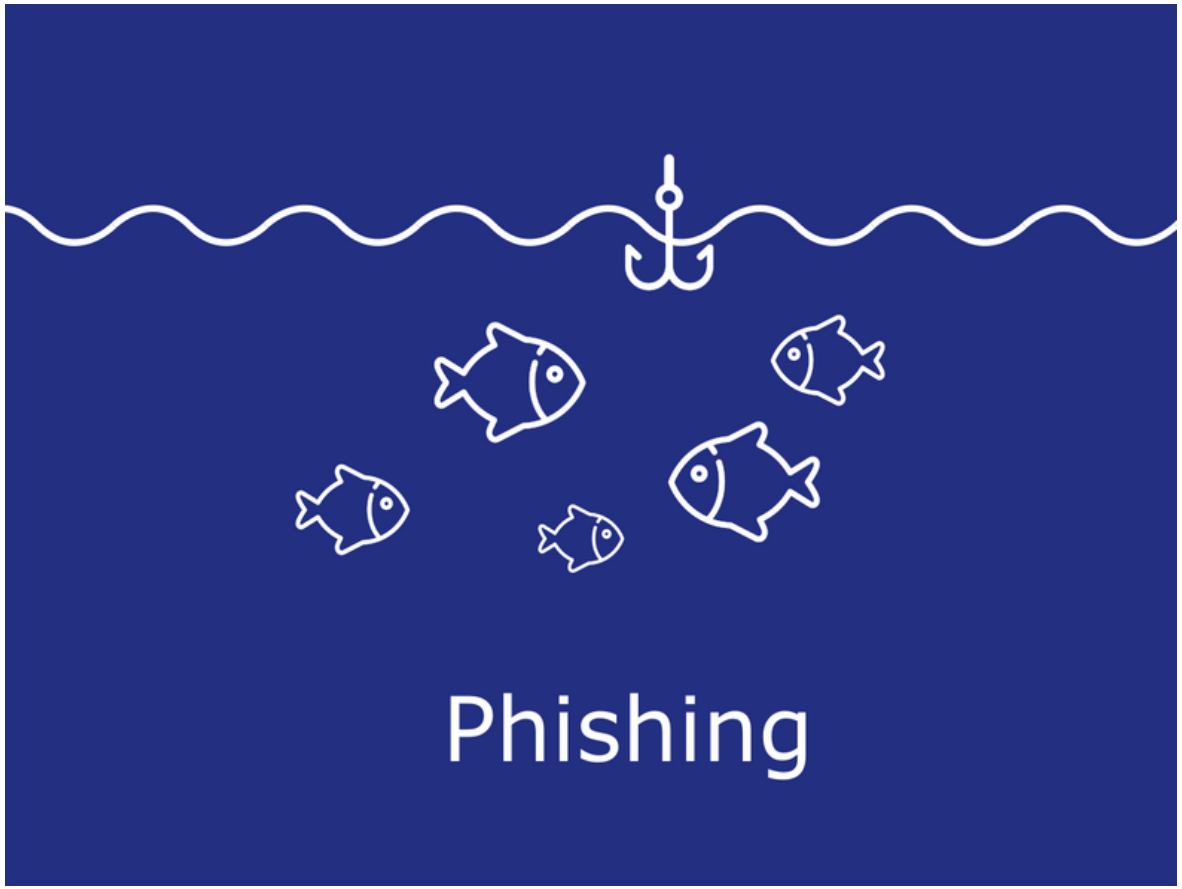
SMShing

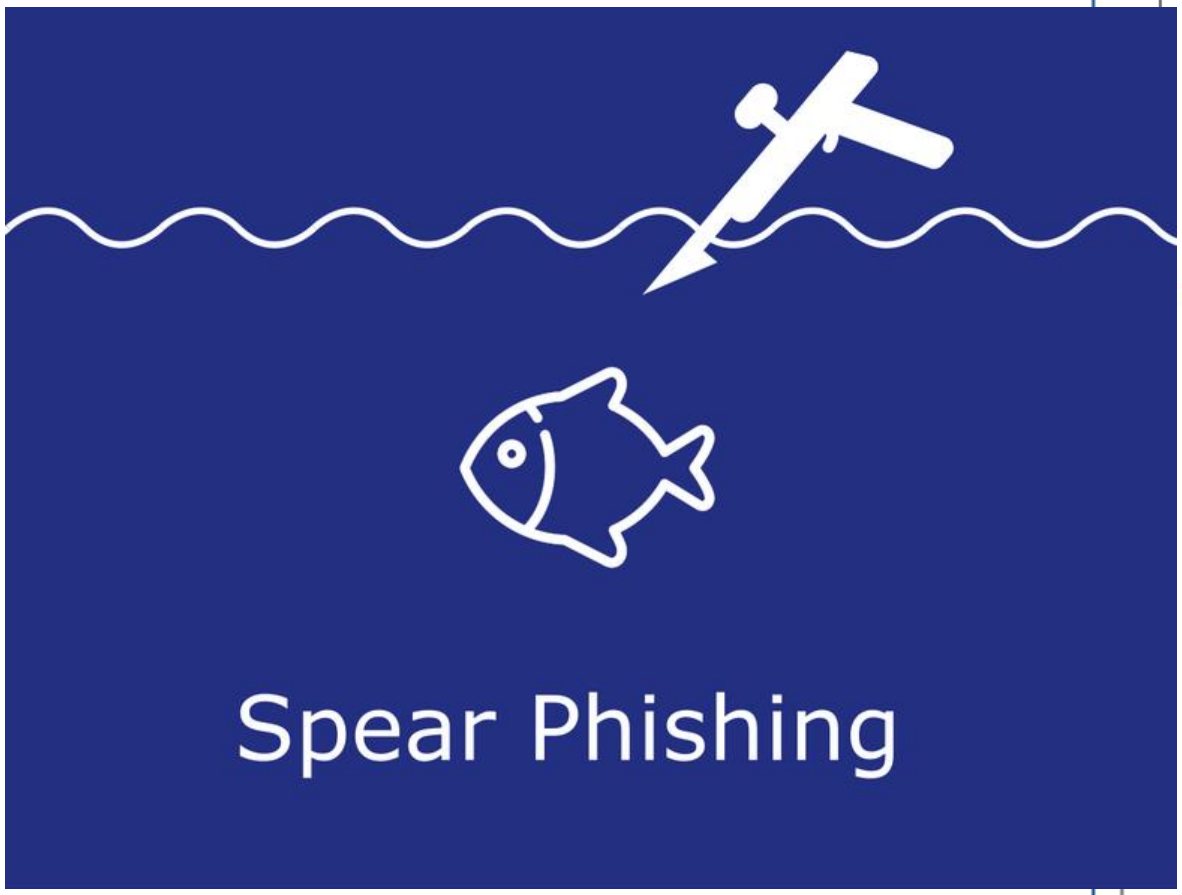


Spear phishing

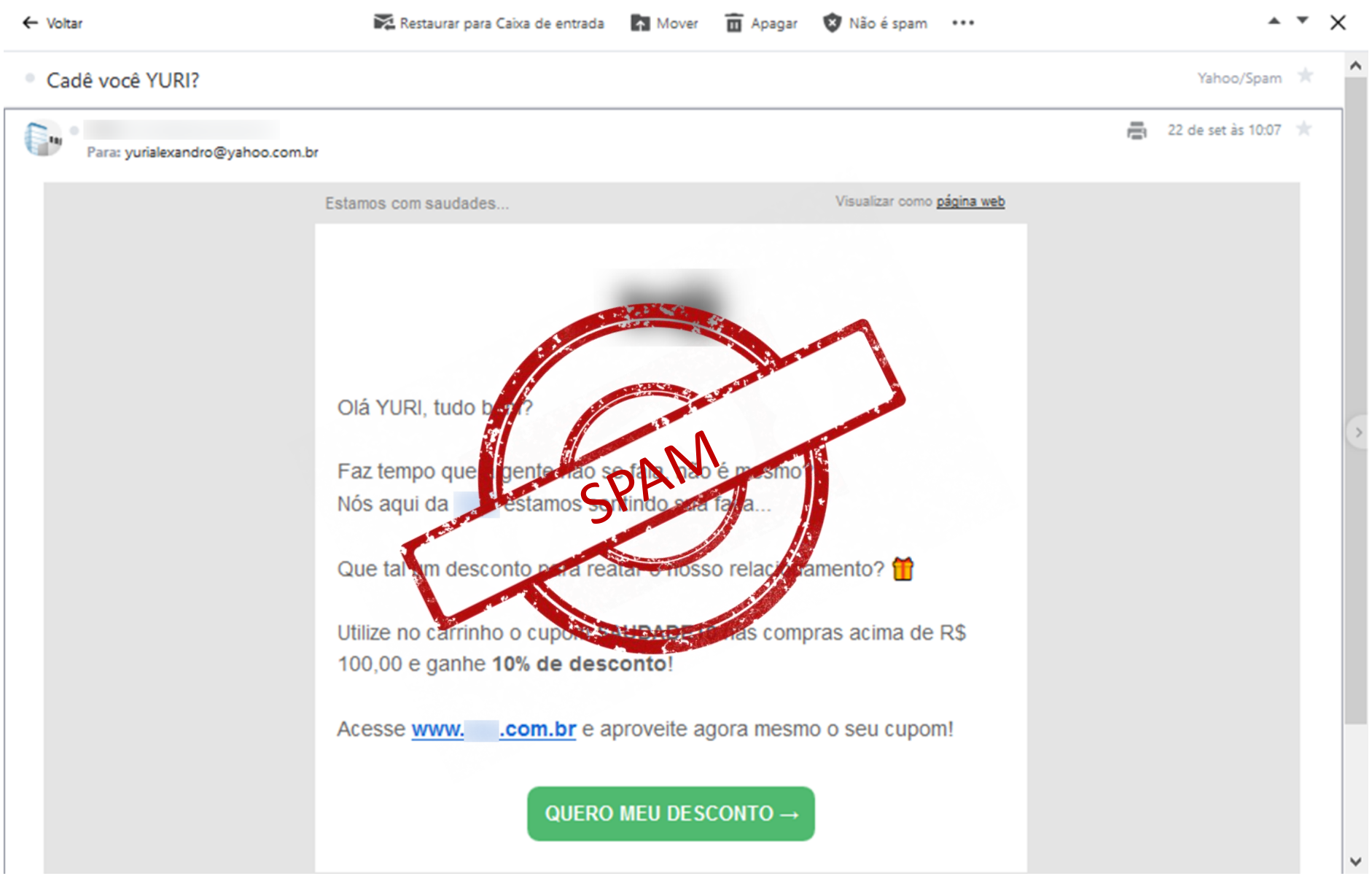


Spear phishing



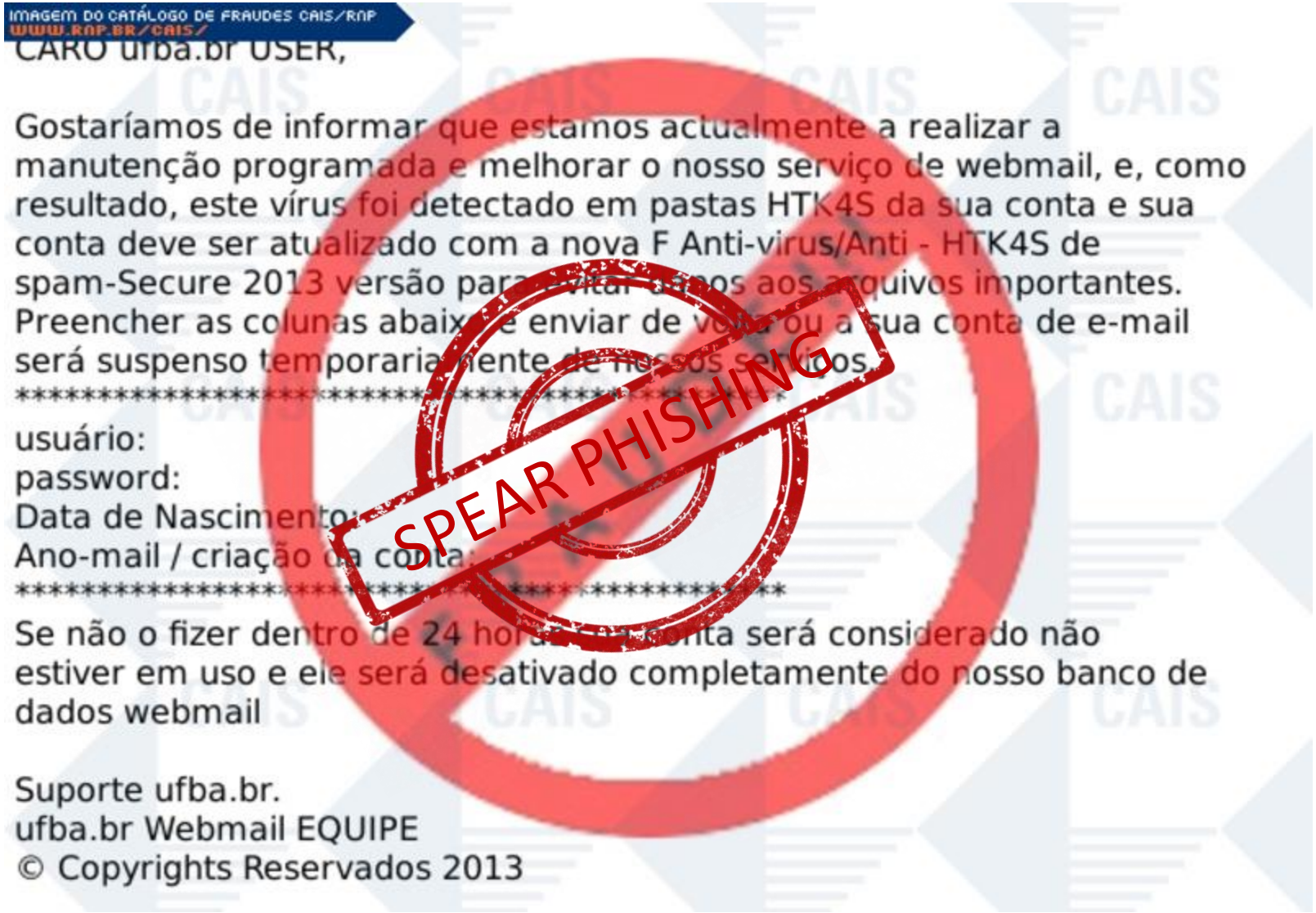


Spear phishing



Spear phishing

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.

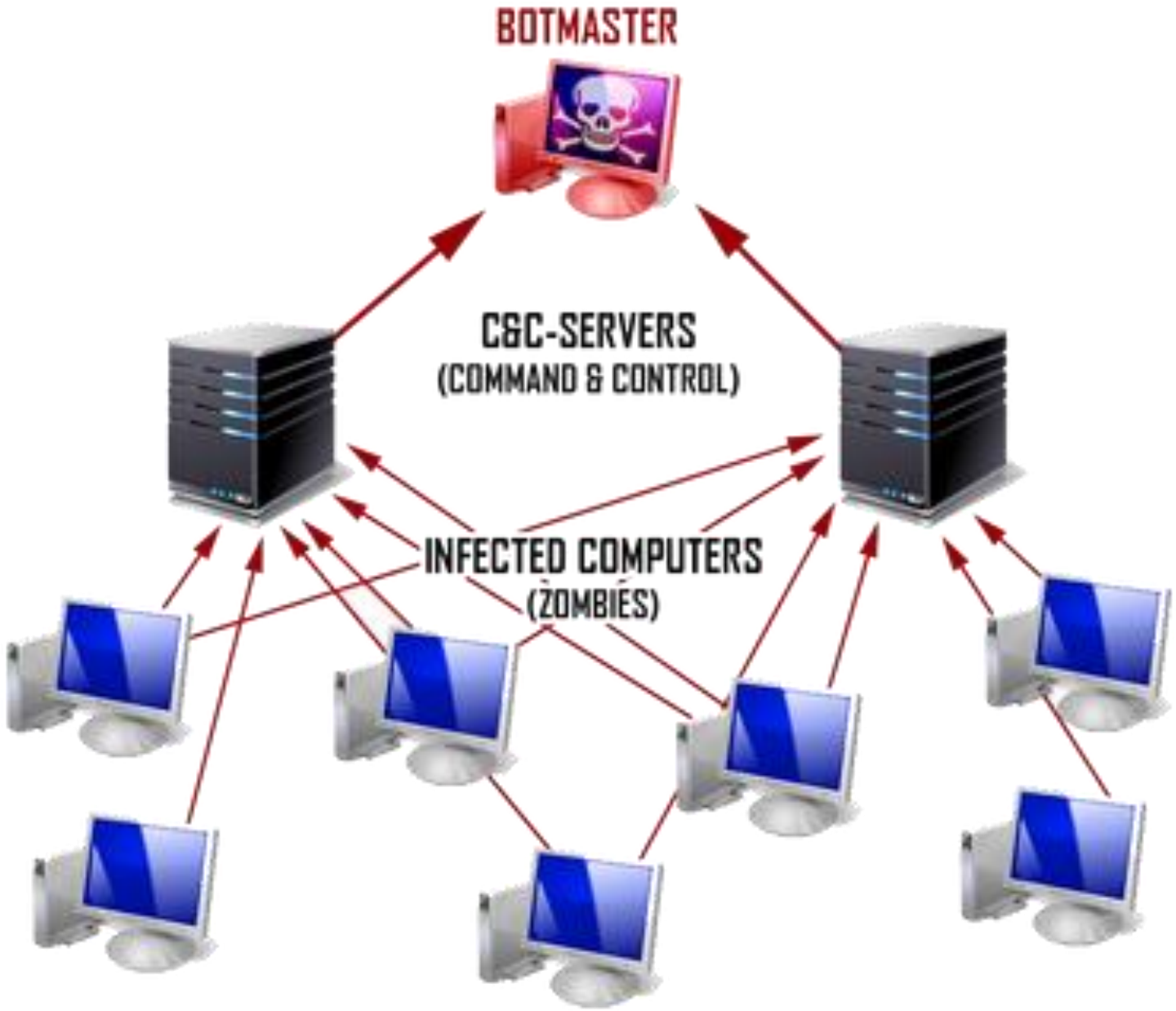
CHEQUE informações sempre que necessário.

Spear phishing

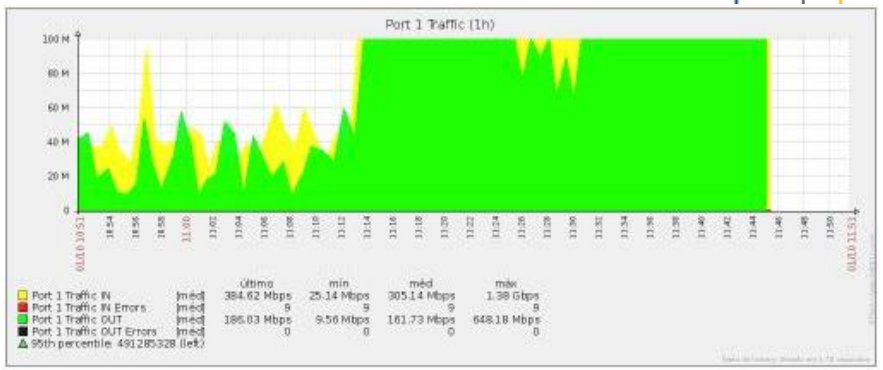
phishing@cais.rnp.br

Botnets

Botnets


BOTMASTER
C&C-SERVERS
(COMMAND & CONTROL)
INFECTED COMPUTERS
(ZOMBIES)

Botnets

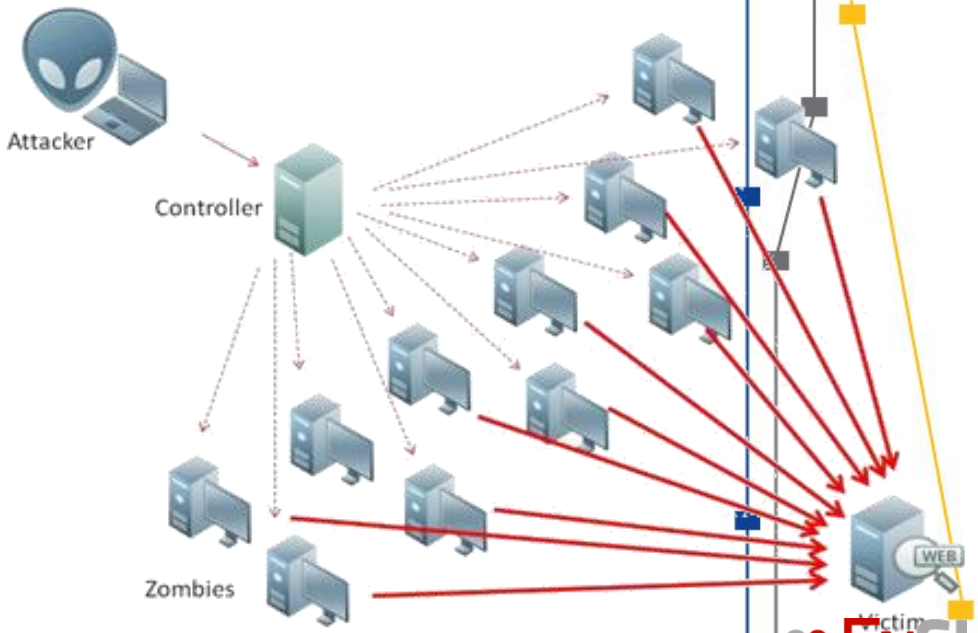


PREJUÍZOS

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.



Botnets

COMO EVITAR

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

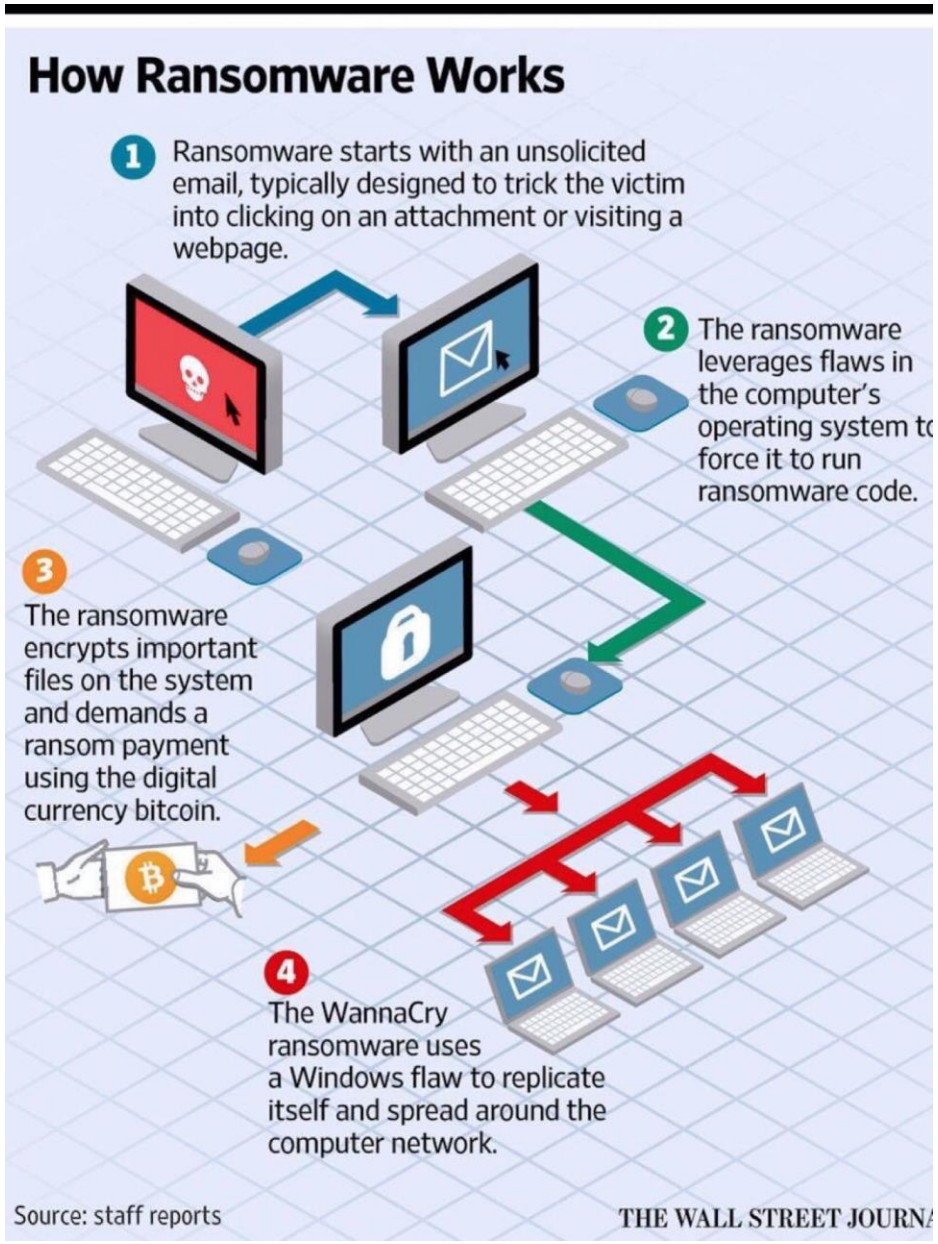
TENHA CUIDADO ao baixar arquivos, não abra e-mails suspeitos.

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.

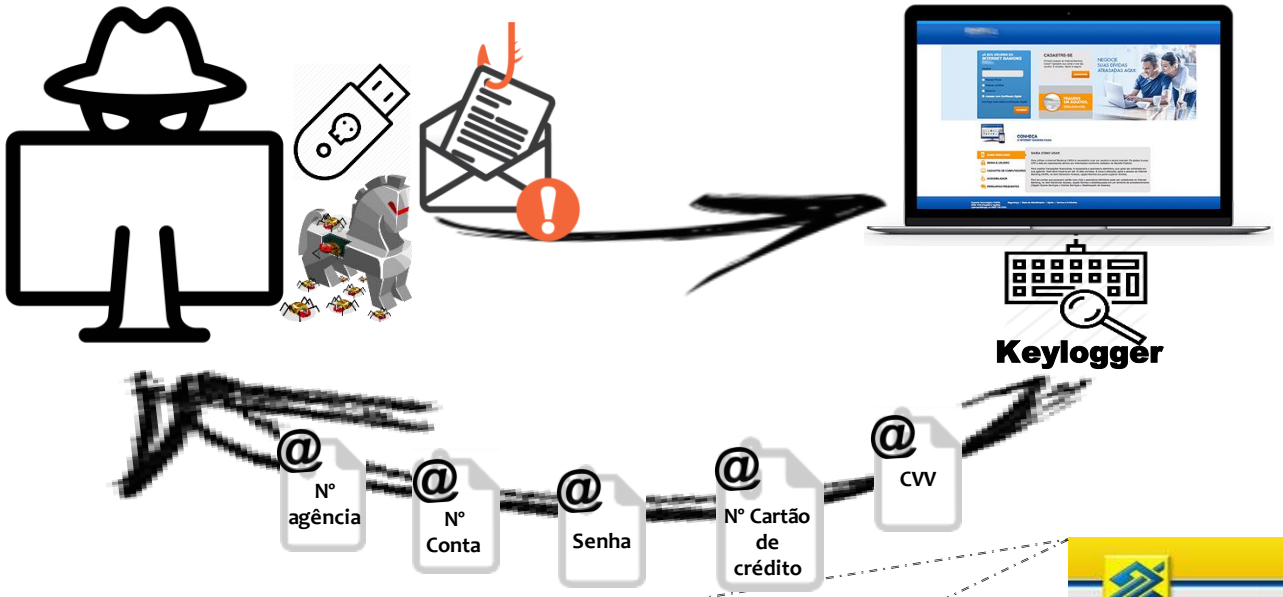
Ransomwares



Fraudes Financeiras

De quantos modos seus dados bancários podem ser roubados?

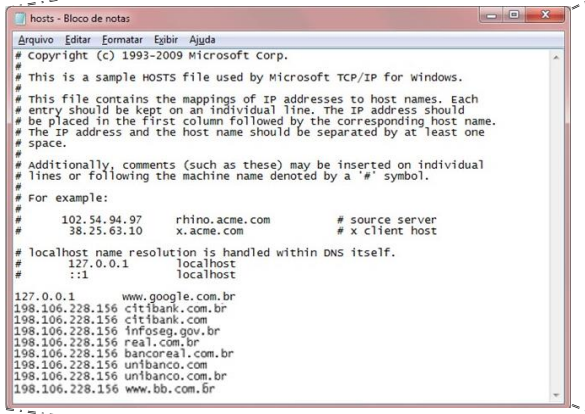
Fraudes financeiras

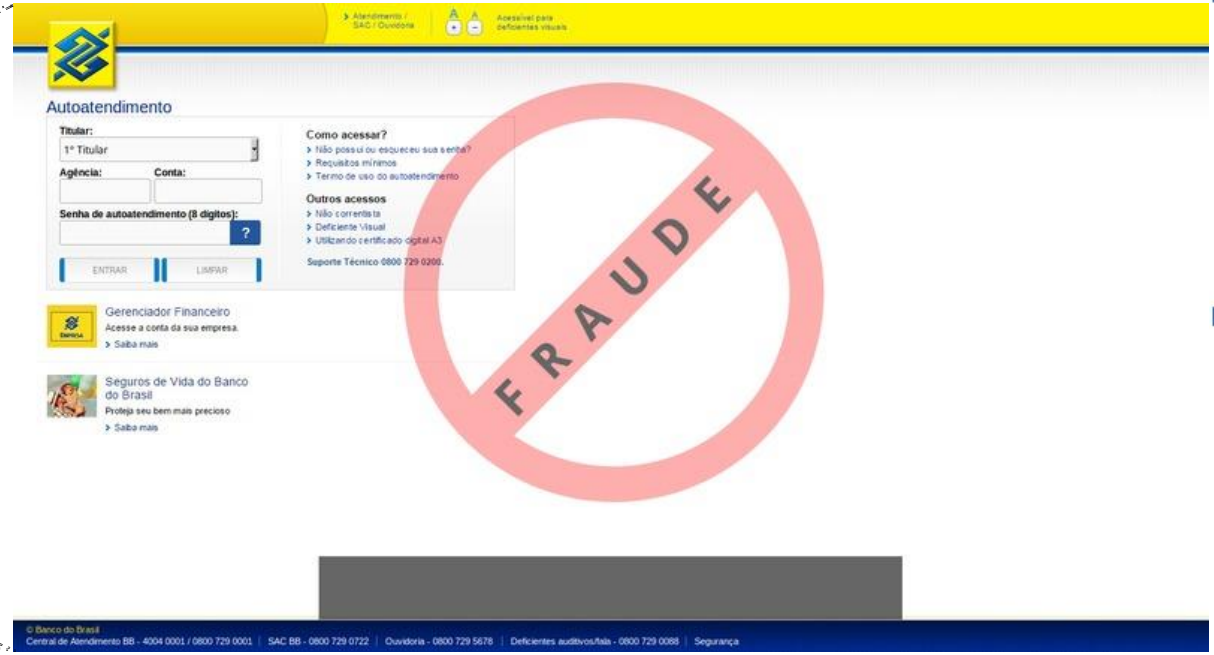


Instalação de malwares

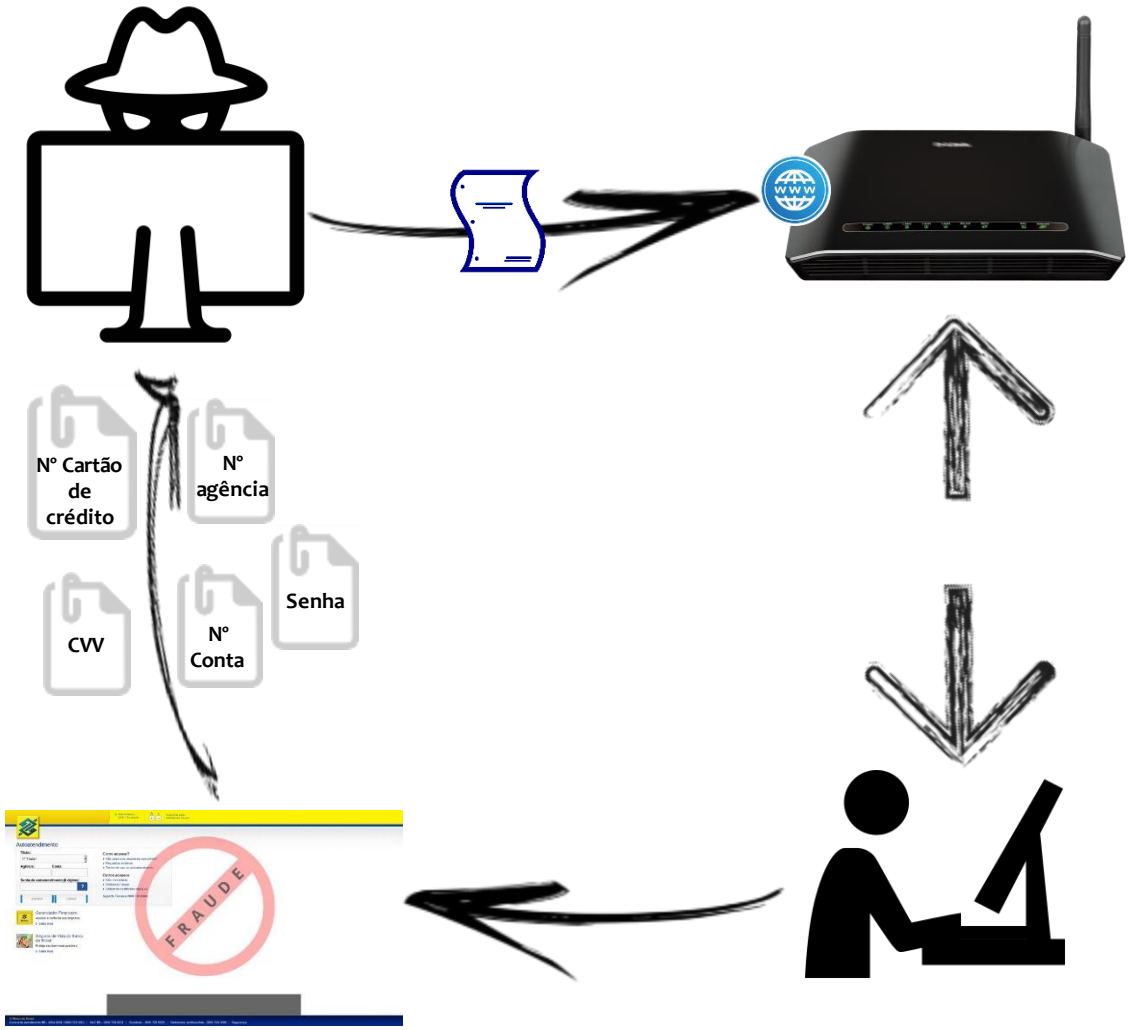
Keylogger

Alteração do arquivo de resolução de nomes (hosts)





Fraudes financeiras



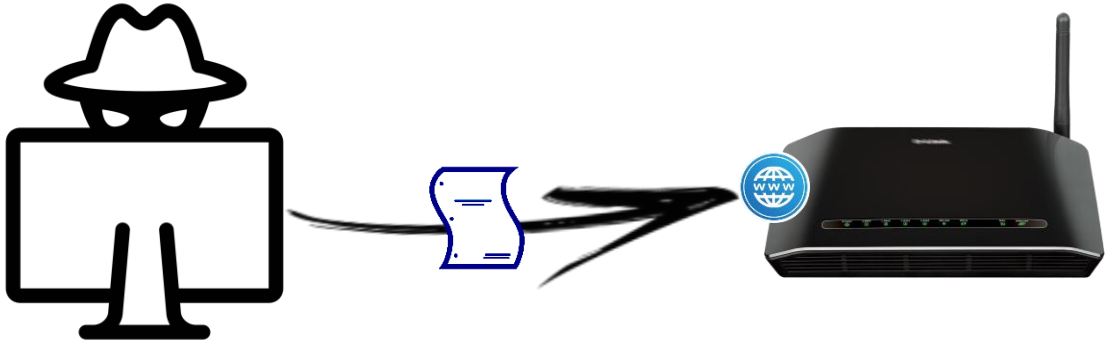
Comprometimento de modems/roteadores ADSL

Alteração do servidor de resolução de nomes (DNS)

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

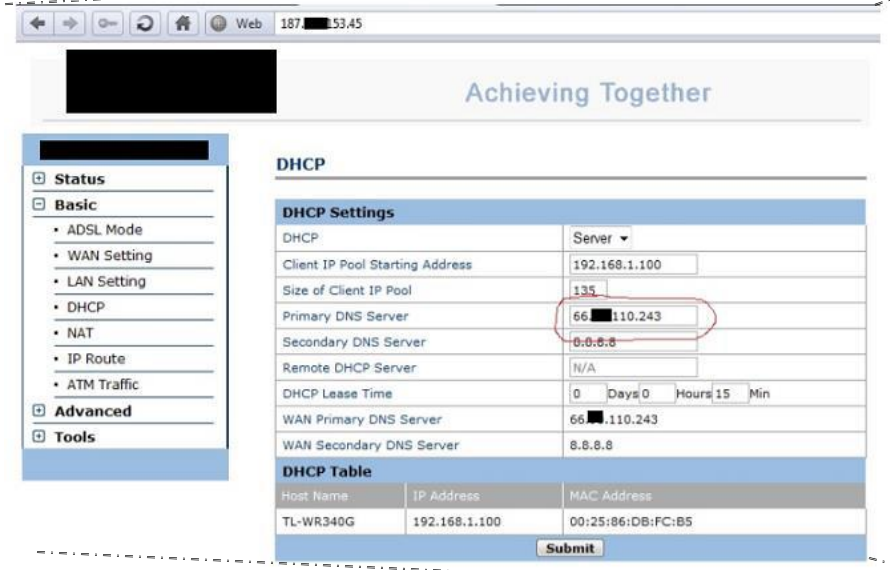
Computador não é comprometido, mas a conexão é maliciosa

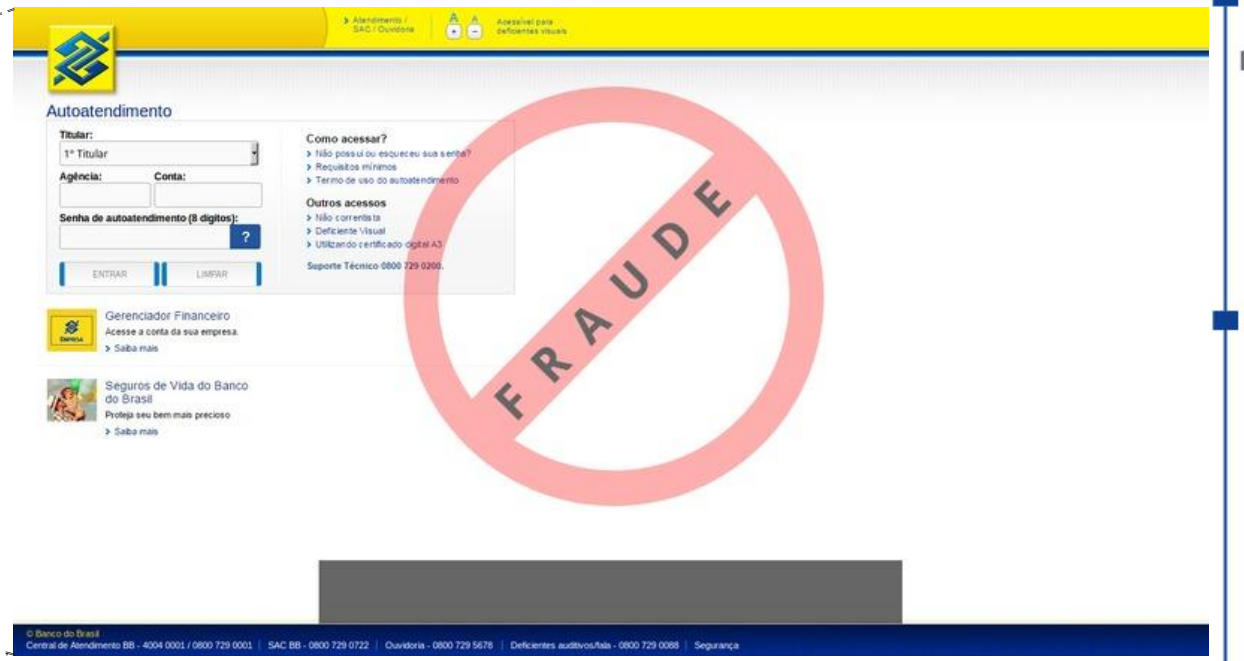
Fraudes financeiras



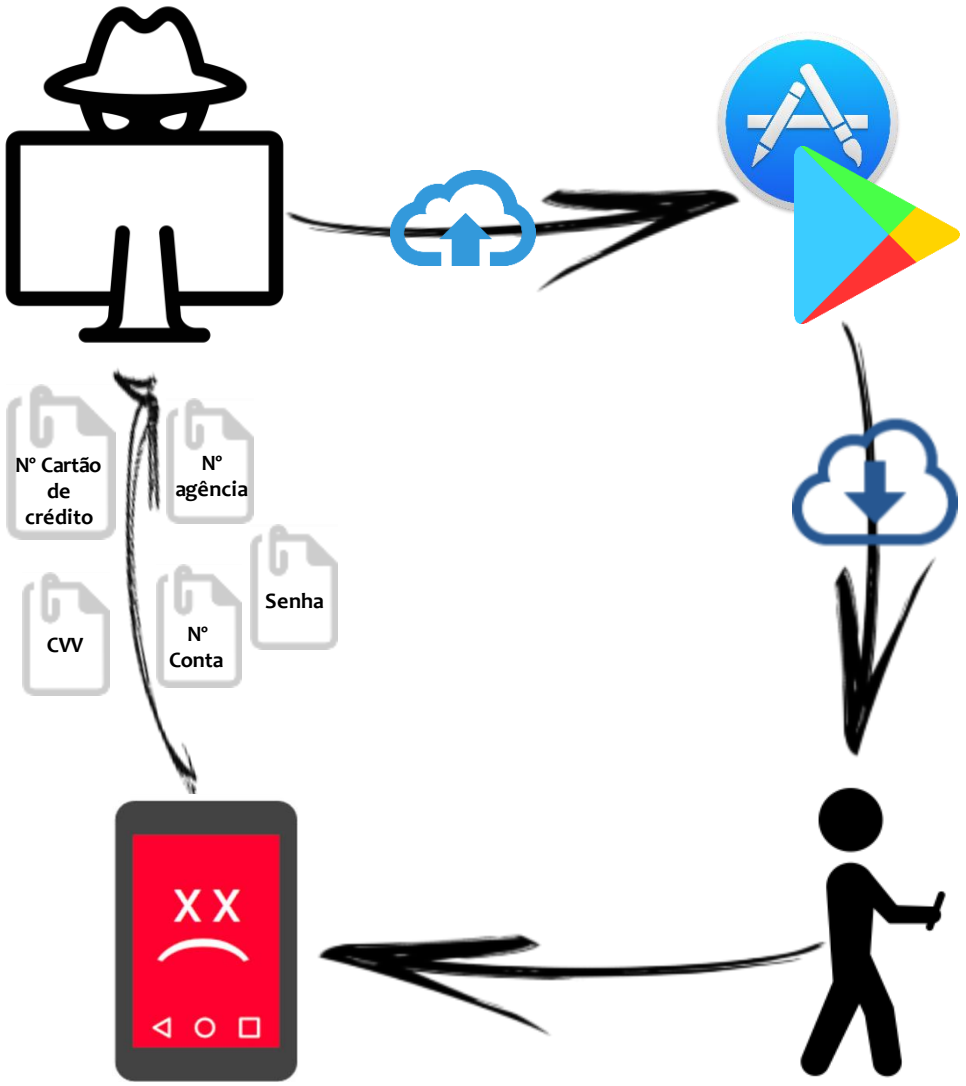
Comprometimento dos modems ADSL

Alteração do servidor de resolução de nomes (DNS)





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

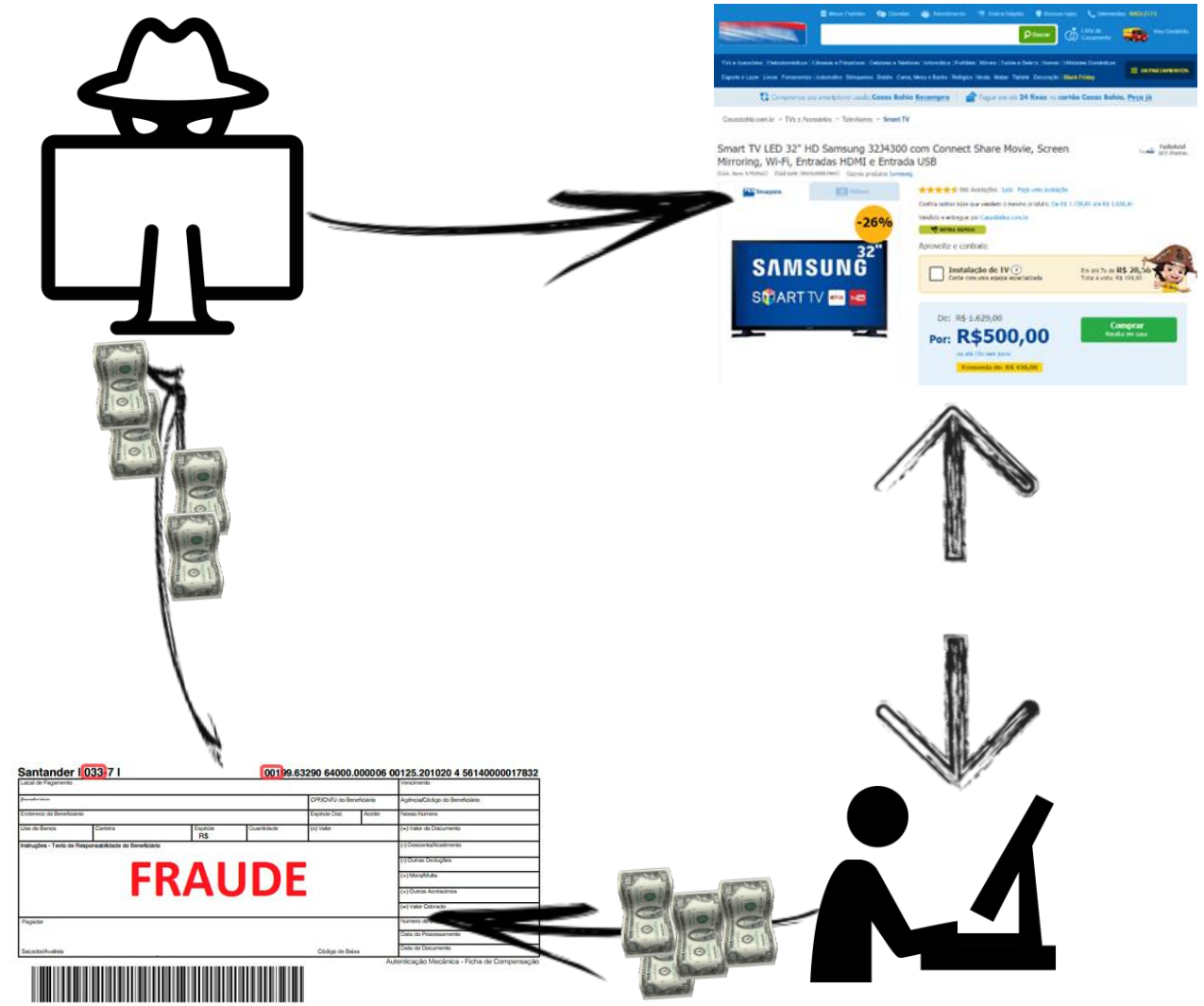
Fraudes financeiras

Apps falsos para tablets/celulares

Fraudes financeiras

Apps falsos para tablets/celulares

Fraudes financeiras



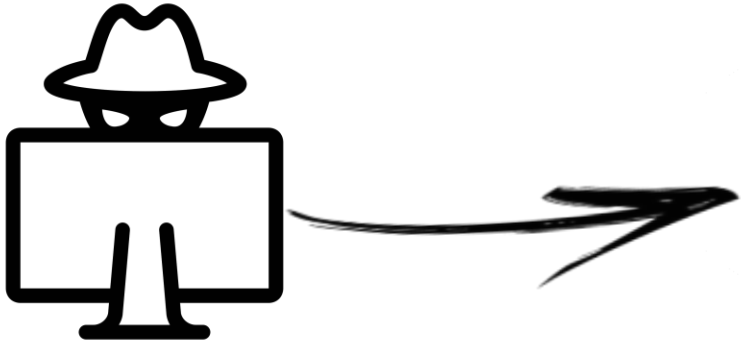
Boletoware

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 39990.82227 68406.019691 83006.330012 5 65160000022663

Local de pagamento: Pagável em qualquer Banco até o vencimento					Vencimento: 30/03/2015
Cedente: Teste LTDA					Agência/Código cedente: 0543 05431218979
Data do documento: 21/07/2015	Nº documento: 0000272539	Espécie doc.: DS	Aceite	Data processamento: 21/07/2015	Nosso número: 18222684060
Uso do banco	Carteira	Espécie: R$	Quantidade: 001	Valor Documento: 226.63	(=) Valor documento: 226.63

Instruções (Texto de responsabilidade do cedente)

- Sr. Caixa, cobrar multa de 2% após o vencimento
- Receber até 10 dias após o vencimento
- Em caso de dúvidas entre em contato conosco: ederson.dev@gmail.com

(-) Desconto / Abatimentos
(-) Outras deduções
(+) Mora / Multa
(+) Outros acréscimos
(=) Valor cobrado

Sacado
João Açunção
Um end. de teste - Bairro-teste
Sobradinho - DF - CEP:73080190

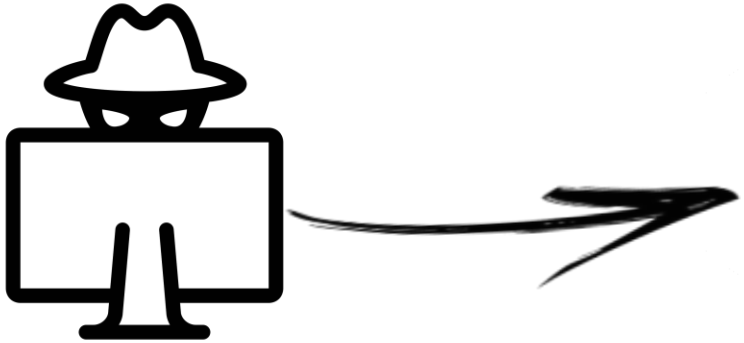
Cód. baixa

Sacador/Avalista

Autenticação mecânica - **Ficha de Compensação**

FRAUDE

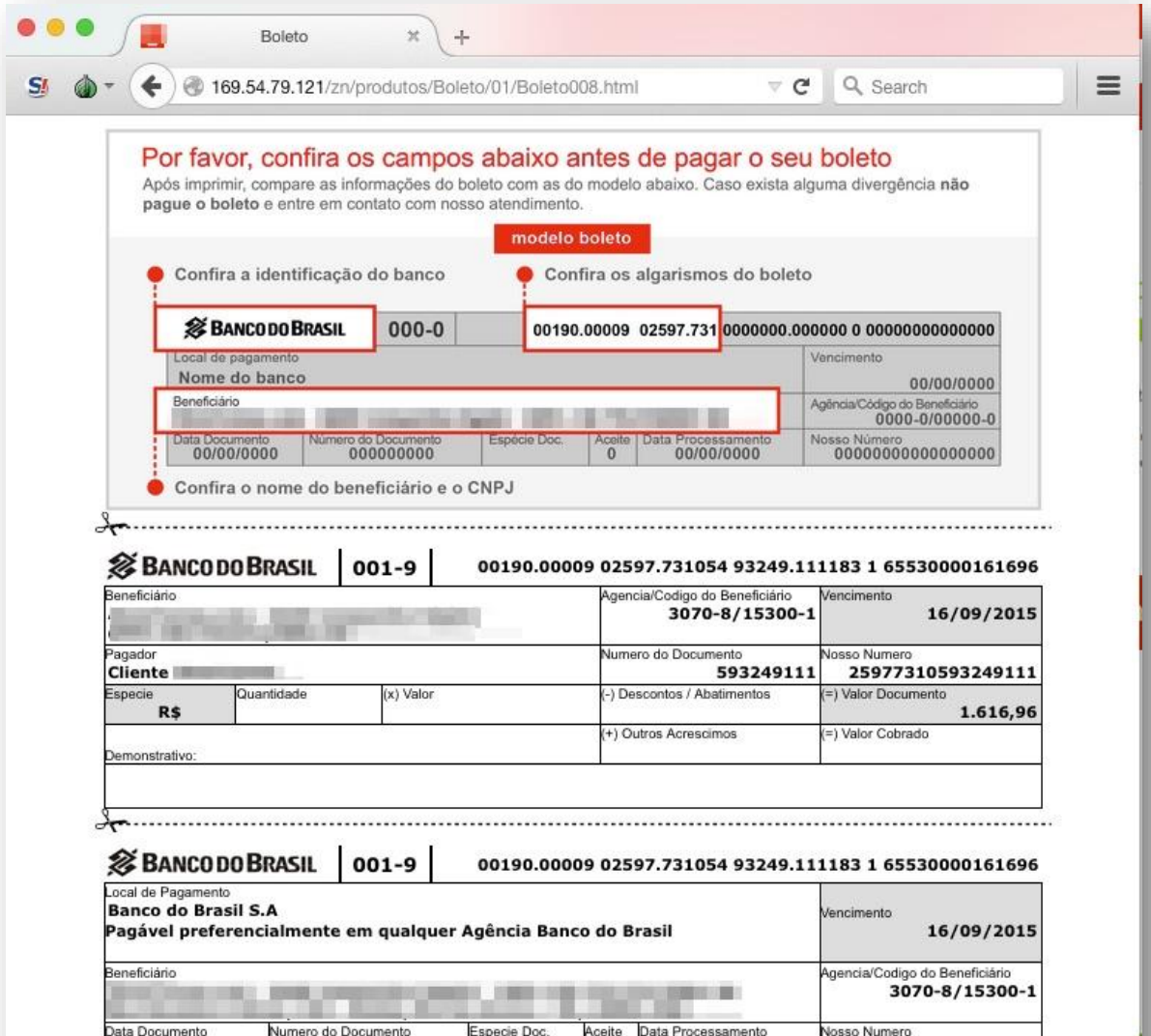
Fraudes financeiras



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



Spear phishing

COMO EVITAR

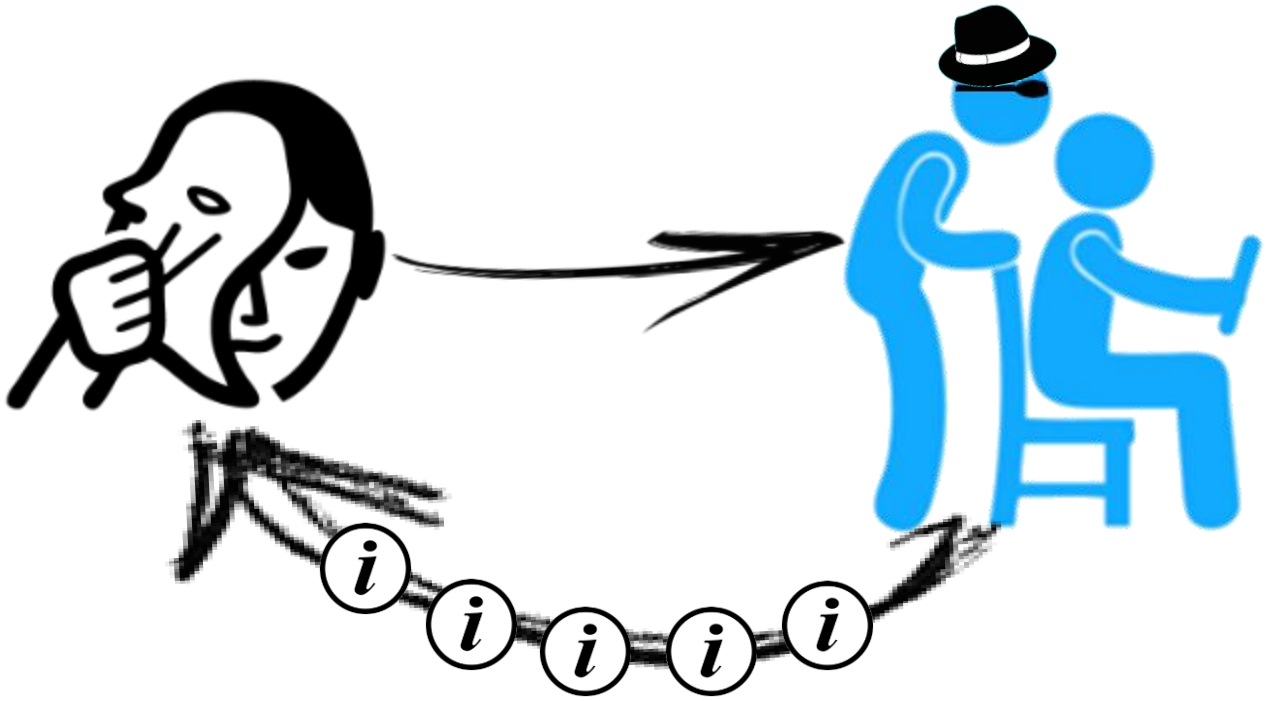
DESCONFIE SEMPRE, EM HIPÓTESE ALGUMA, NUNCA, CHEQUE...

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.

Engenharia Social

Email – Yuri Alexandro – Outlook - Mozilla Firefox

https://outlook.live.com/mail/deeplink 90%

Doc Eletronico 777552244

Sylvia Mara <[redacted]@hotmail.com>
Qua 26/09/2018, 08:09
Você

-DOC-Eletronico.html.ht...
9 KB

Baixar Salvar no OneDrive

DOC.pdf

2 anexos (total de 155,2 KB)

Baixar tudo como zip

Antes de tudo, gostaria de me desculpar pela demora em dar um retorno, eu tive alguns contratempos em casa e acabei me atrasando.

Efetuei o DOC - Eletrônico, dia 26/09/2018 , no valor de R$1.142,55

Perdoe-me pelo inconviniente, peço para que verifique e me dê um retorno no máximo até amanhã às 10:00 pois estarei saindo de férias.

Desde já, agradeço.

Caso não consiga visualizar os anexos corretamente, acesse aqui

ENSI

MÊS de SEGURANÇA

CAIS RNP

Engenharia Social

“A arte de enganar”

VÍDEO

https://youtu.be/QskBef2mGnU

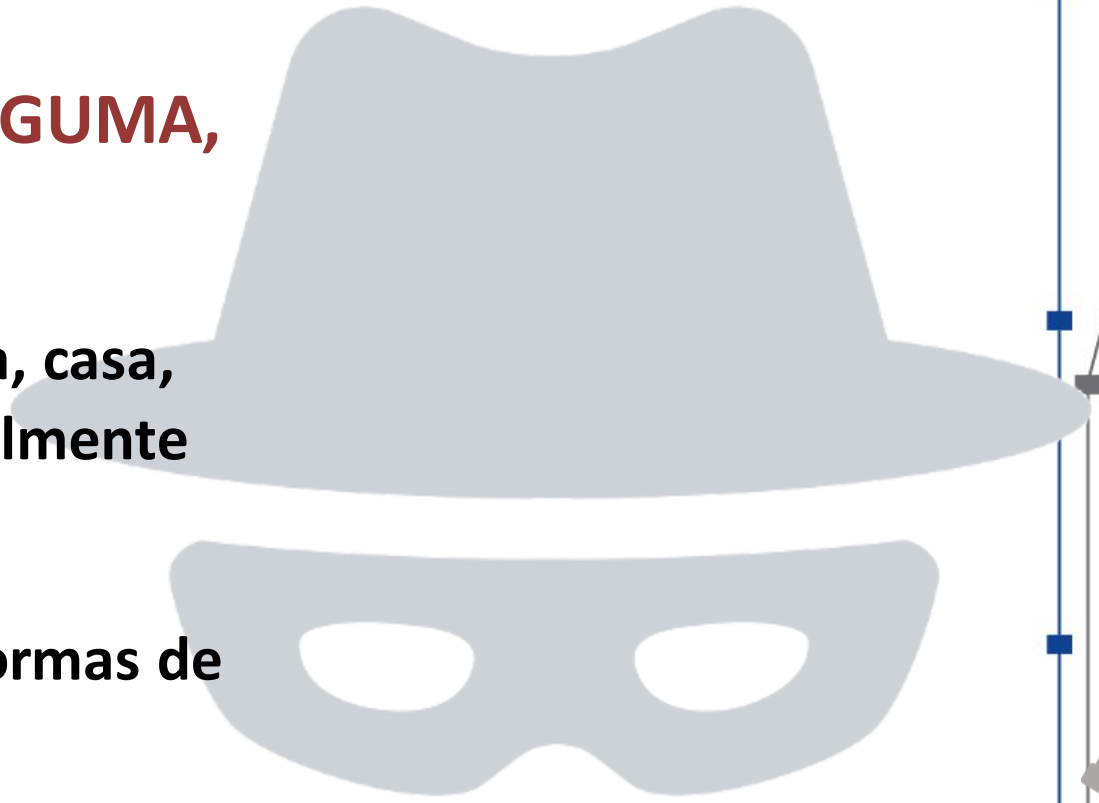
Engenharia Social

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.



Engenharia Social

VÍDEO

https://youtu.be/WaI6Z6MEMew

RNP

sd@rnp.br

0800 722 0216

(61) 9 9960 5971

1916*800

cais@cais.rnp.br

RNP

MINISTÉRIO DA DEFESA

MINISTÉRIO DA CULTURA

MINISTÉRIO DA SAÚDE

MINISTÉRIO DA EDUCAÇÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES

BRASIL GOVERNO FEDERAL