CARTILHA CONTRA CRIMES VIRTUAIS

GOVERNO DO ESTADO
RIO DE JANEIRO

CARTILHA CONTRA CRIMES VIRTUAIS

Durante a pandemia da Covid-19, o universo virtual cresceu muito. Passou a ser o principal canal para se pedir comida, fazer compras, se comunicar, realizar operações bancárias... enfim, todos passaram a usar mais a internet.

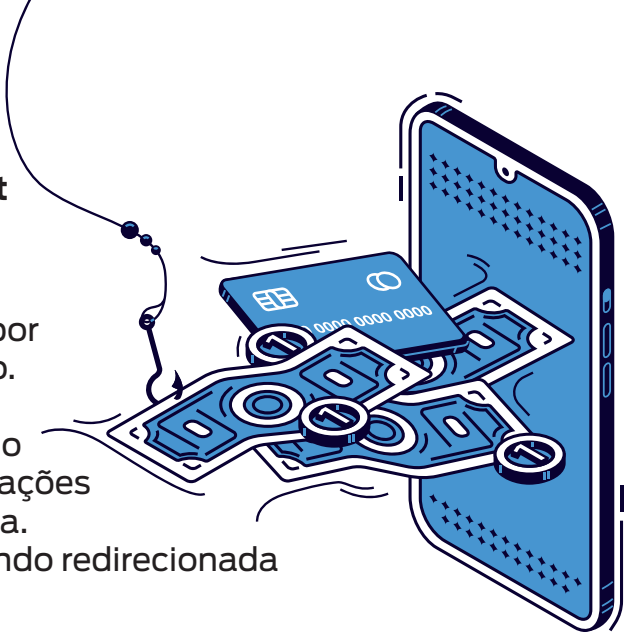
Mas se esta já era a realidade para algumas pessoas, para outras passou a ser um novo mundo, cheio de novidades e dúvidas. E aproveitando este cenário, os estelionatários passaram a aplicar golpes usando as redes. O Instituto de Segurança Pública (ISP) chegou a registrar aumento de 273% neste tipo de crime entre os meses de março e agosto, número quase quatro vezes maior quando comparado ao mesmo período do ano passado.

Para ajudar os cidadãos, o Governo do Estado acionou os especialistas do Procon e da Polícia Civil para oferecer dicas que podem evitar muitos problemas, como roubo de senhas, invasão de rede social, pagamento de boletos falsos ou qualquer outro tipo de estelionato virtual.

PROCONRJ
Secretaria de Polícia Civil
GOVERNO DO ESTADO
RIO DE JANEIRO

CONHEÇA O “PHISHING”

Um dos golpes mais comuns da internet



Criminosos costumam enviar mensagens (e-mails, SMS, WhatsApp) se passando por empresas privadas e bancos, por exemplo.

Nessas mensagens, é solicitado ao usuário que execute arquivos para efetuar atualizações ou que confirme informações de sua conta.
Ao clicar no endereço, a pessoa acaba sendo redirecionada para uma página falsa que irá:

roubar as informações inseridas
ou
instalar um vírus no seu dispositivo.

QUATRO DICAS SIMPLES PARA NÃO SER VÍTIMA:

1 - Nunca abra anexos ou links de mensagens não solicitadas.

2 - Nunca forneça suas informações pessoais.

3 - Mantenha o seu navegador, antivírus e sistema operacional sempre atualizados.

4 - Sempre confira se o endereço acessado é realmente o endereço correto.

CONHEÇA UM DOS MÉTODOS MAIS UTILIZADOS PARA FURTAR SENHAS

Criminosos convencem as vítimas a clicar em uma mensagem enviada por eles sob o pretexto de receber algum benefício.

Quando a vítima clica, ela é redirecionada para uma página falsa, porém idêntica àquela que está habituada a acessar.

Ao inserir usuário e senha para entrar na página, os dados são capturadas pelo criminoso.

Em seguida, é exibida uma mensagem de erro e o usuário é redirecionado à página verdadeira da rede social.

Deste modo, o criminoso tem acesso à rede social da vítima, que não percebe que sofreu um golpe virtual.

CONHEÇA O GOLPE USADO PARA INVADIR O SEU WHATSAPP

Exemplo de QR CODE

1

O aplicativo WhatsApp também pode ser utilizado no computador: o **WhatsApp Web**.

Para que isso seja possível, o usuário tem que utilizar o seu aparelho celular para ler um **código QR** gerado pela página oficial do aplicativo.

Criminosos clonam a página oficial do aplicativo e expõe um código QR falso que faz com que possam monitorar ou clonar o WhatsApp da vítima. Isso acontece mais em redes compartilhadas.

COMO CONFIRMAR SE ESSE MONITORAMENTO ESTÁ ATIVO?

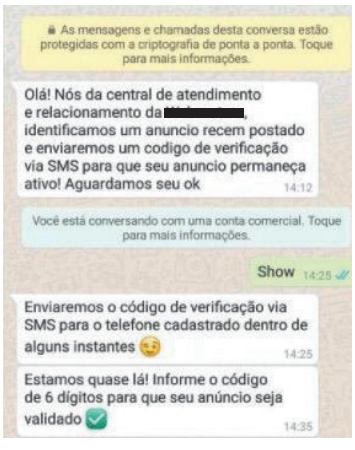
- dentro do aplicativo, selecione os três pontos no canto superior direito e a opção WhatsApp Web.

- caso apareça a mensagem última sessão ativa ou ativo agora, significa que alguém ativou o acesso web no seu telefone.

- para desativar, basta selecionar a opção '**sair de todas as sessões**'.

ATENÇÃO:
Não utilize o seu aparelho para ler códigos enviados por estranhos!

2



No caso de pessoas que divulgaram seus celulares em sites de vendas, pode ocorrer o seguinte golpe:

Com o número do seu telefone em mãos, o criminoso tenta habilitar o seu WhatsApp em outro aparelho, mas isto **só é possível com o uso de uma senha que é enviada por SMS.**

Neste momento, o golpista entra em contato com a vítima, se passando por funcionário do site. Ele explica que será enviado um **SMS** com uma senha e solicita os números para validar o anúncio.

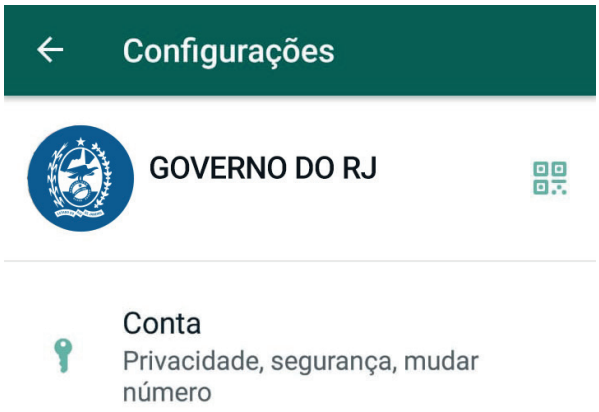
Assim que a vítima informa o código, os criminosos passam a ter controle sobre o seu WhatsApp. Passando-se pela vítima, pedem dinheiro para todos os seus contatos.

VEJA O PASSO A PASSO PARA DAR MAIS SEGURANÇA AO SEU WHATSAPP - ANDROID

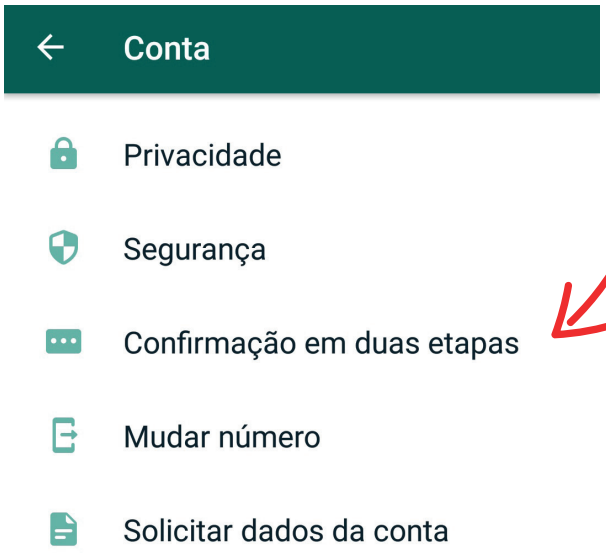
Ative a confirmação em duas etapas!

1 - Dentro do aplicativo, selecione os três pontos no canto superior direito.

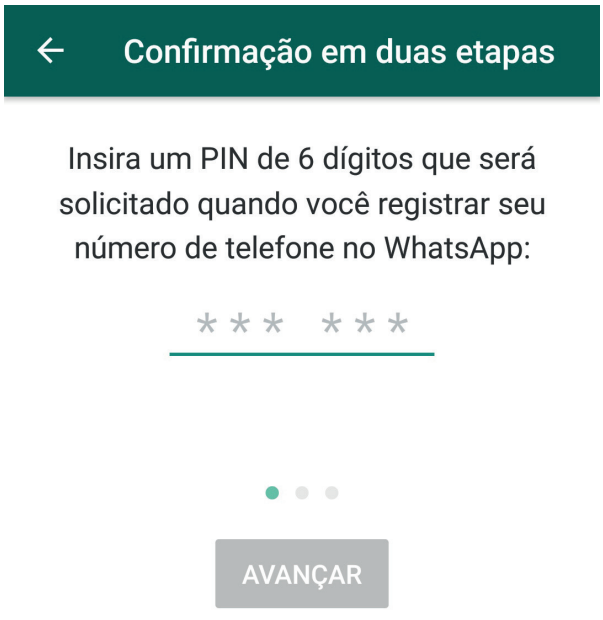
2 - Selecione “configurações” e depois “conta”.



3 - Aperte em ativar na opção **“confirmação em duas etapas”**;



4 - Crie o PIN de 6 dígitos e pronto! Agora a sua conta de WhatsApp está mais segura!



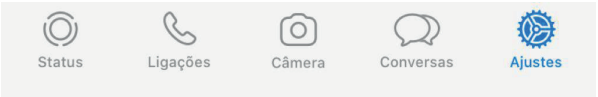
ATENÇÃO:

É muito importante memorizar esse PIN, porque, de vez em quando, ele será solicitado pelo aplicativo!

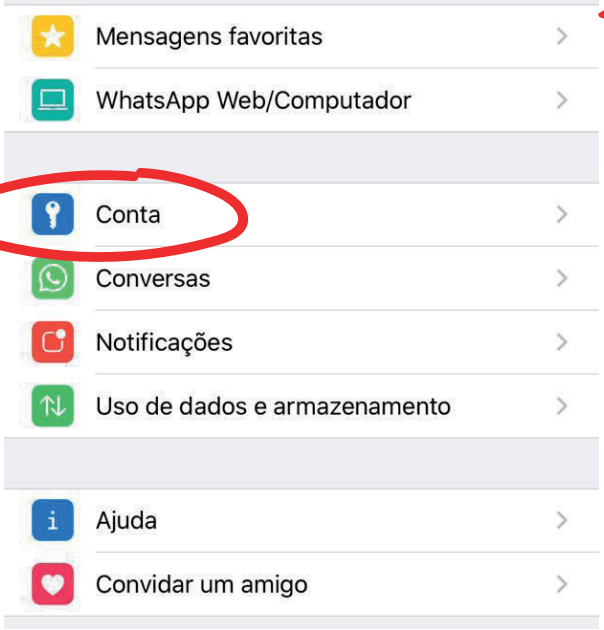
VEJA O PASSO A PASSO PARA DAR MAIS SEGURANÇA AO SEU WHATSAPP - IOS

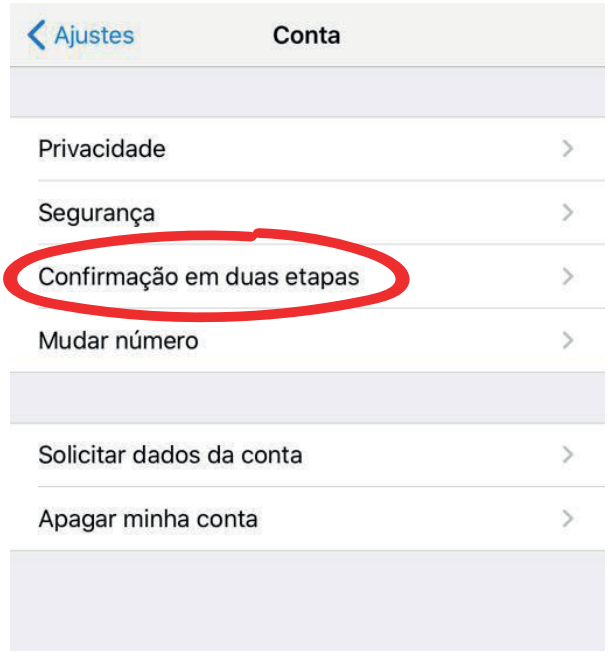
Ative a confirmação em duas etapas!

1 - Dentro do aplicativo, selecione “ajustes” no canto inferior direito.



2 - Selecione “conta” e depois “confirmação em duas etapas”





3 - Aperte em “ativar”

4 - Crie o PIN de 6 dígitos e pronto! Agora a sua conta de WhatsApp está mais segura!

ATENÇÃO:

É muito importante memorizar esse PIN, porque, de vez em quando, ele será solicitado pelo aplicativo!

CONHEÇA OS LINKS ENCURTADOS E SAIBA COMO EVITAR GOLPES EM QUE ELES SÃO USADOS

Links podem gerar endereços de internet muito grandes.
Ex:
http://www.rj.gov.br/NoticiaDetalhe.aspx?id_noticia=9182

Para facilitar a divulgação destes links, existem páginas na internet que encurtam links para facilitar o seu compartilhamento.
Ex:
https://bitly.com/ https://tinyurl.com/ https://t2mio.com/

Usando um dos encurtadores acima, o endereço:
http://www.rj.gov.br/NoticiaDetalhe.aspx?id_noticia=9182

se transforma em: https://bit.ly/3kUTsRl

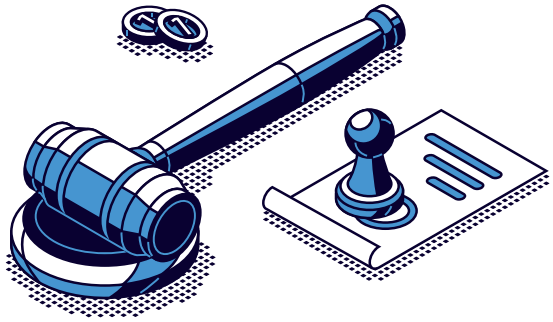
Desta forma, o usuário não tem como identificar, por exemplo, que o link se refere a uma notícia do site do Governo do Estado. Ou seja, não é possível saber para onde o cidadão será direcionado com a simples leitura do endereço fonte, que no caso da notícia é http://www.rj.gov.br.

Sendo assim, tenha muito cuidado com endereços encurtados.

O SERVIÇO PODE SER USADO POR ESTELIONATÁRIOS PARA DAR GOLPES VIRTUAIS.

CONHEÇA OS GOLPES DE LEILÕES NA INTERNET

Existem diversas páginas falsas de leilão na internet. Saiba como evitar ser vítima de um estelionato virtual:



Evite páginas que não sejam ".com.br";

Se o bem oferecido pertencer a um órgão público, cheque no site do departamento ou empresa pública se realmente o leilão está para ocorrer.

Procure referências sobre as páginasde leilão em sites com boa reputação, como o portal "**Reclame Aqui**" ou "**E-bit**";

Não transfira dinheiro para a conta de uma pessoa física. Empresas reais são obrigadas a possuir um CNPJ. Busque informações sobre a empresa na internet;

Antes de pagar o lance, tente ir pessoalmente ao local onde ocorre o leilão.

COMPRAS COM SEGURANÇA

Confira as principais dicas para realizar a compra on-line com segurança.

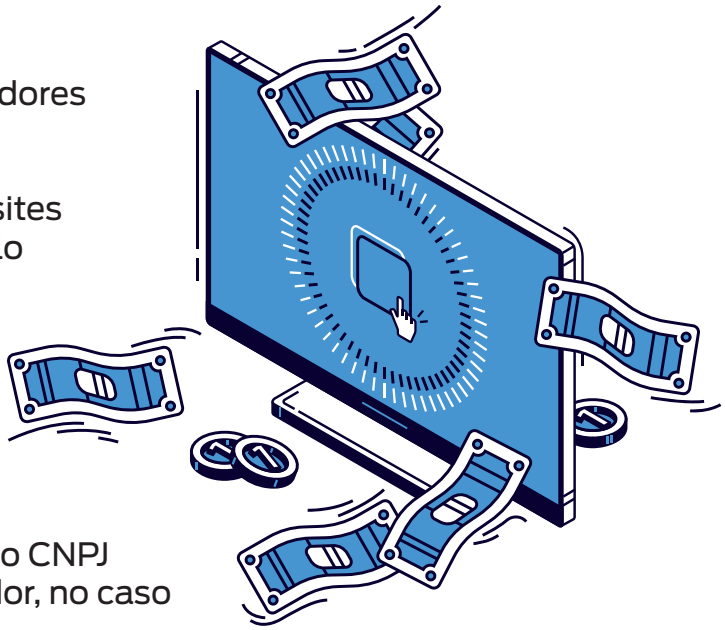
Dicas básicas:

· Sempre desconfie de valores muito abaixo do mercado. Há uma boa chance de ser um golpe ou um produto roubado;

· Evite comprar de lojas ou vendedores desconhecidos;

· Confira a reputação da loja em sites especializados, como por exemplo o “Reclame Aqui” ou o “E-bit”.

· Verifique se o site é seguro.



Antes de comprar, verifique:

· O nome comercial e o número do CNPJ da empresa. Ou o CPF do vendedor, no caso de pessoa física;

· O contato do SAC ou Ouvidoria;

· As informações necessárias para a localização e contato do fornecedor, como endereço físico e eletrônico;

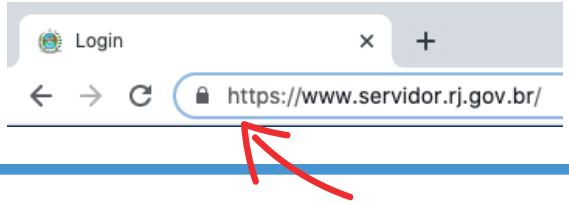
· Havendo dúvida, o consumidor pode consultar os dados digitando o CNPJ da empresa no site da Receita Federal (http://servicos.receita.fazenda.gov.br/Servicos/cnpjreva/Cnpjreva_Solicitacao.asp).

· De preferência a digitar o endereço eletrônico da empresa ou instituição para obter um boleto ou segunda via para pagamento. Evite direcionamentos na busca pela internet.

ATENÇÃO:

Os fraudadores costumam criar sites falsos e com aparência profissional para atrair vítimas.

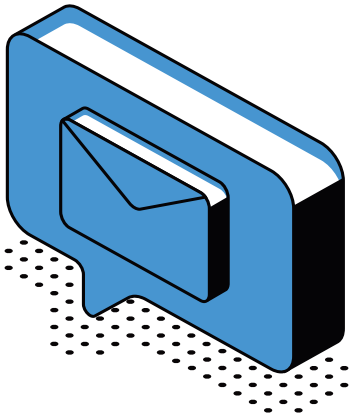
Os endereços eletrônicos que possuem certificado digital e selo de segurança começam com “**HTTPS**” e também um ícone em forma de **cadeado fechado**.



CUIDADO COM LINKS E E-MAILS RECEBIDOS

· Não instale aplicativos de origem desconhecida, ou por meio de links recebidos em serviços de mensagens;

· O ideal é acessar a loja de aplicativos do seu celular (Google Play ou Apple store), e baixar por esse caminho. Muitos golpistas criam links e aplicativos falsos, parecidos com os reais, para aplicar golpes;



· **Atenção ao receber links e boletos por e-mail.** Verifique se o endereço que aparece após o @ é o site oficial da empresa.

Ex.
financeiro@NomeDaLoja.com.br.

· Ao pagar um boleto, verifique se o **código de barras** começa pelo **número do seu banco** (cada banco tem um número próprio).

· Desconfie de valores muito diferente (acima ou abaixo) daqueles que costuma pagar por um serviço ou uma mensalidade. Na dúvida, ligue para o serviço de atendimento da empresa ou instituição.

DESCONFIE SEMPRE

· Sites com preços muito abaixo do mercado merecem atenção dobrada!

· Em caso de dúvida, não compre e entre em contato com o Serviço de Atendimento ao Consumidor (SAC) da empresa solicitando informações;

· Suspeite de mensagens de instituições financeiras solicitando confirmação de dados ou oferecendo pontos de programas de fidelidade.

ATENÇÃO COM AS COMPRAS PELO WHATSAPP E REDES SOCIAIS

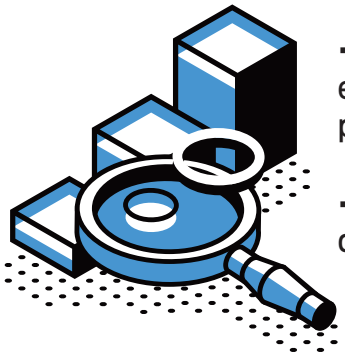
· Não é recomendável que os consumidores finalizem as compras pelas redes sociais, mas sim por meio de um **site seguro** e confiável;

· Antes de comprar por aplicativo de troca de mensagens instantâneas como o WhatsApp, veja se o número pertence à empresa.

Pesquise antes!

VERIFIQUE A REPUTAÇÃO DA EMPRESA

· Ao comprar em sites desconhecidos, é importante pesquisar o que outros consumidores relataram sobre a empresa nas redes sociais. Conhecer a opinião dos outros é uma forma de consultar a reputação do vendedor.



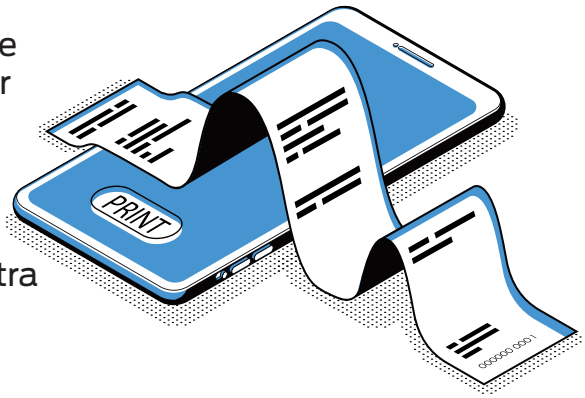
· Jamais insira dados pessoais - como nome, CPF, endereço e número de cartões - em página de pagamento de uma empresa desconhecida;

· Não forneça os dados pessoais para **qualquer e-mail** que chegue na caixa de entrada.

GUARDE OS COMPROVANTES DAS COMPRAS

· Ao efetuar compras on-line, é importante capturar todas as telas (“**prints**”), e salvar o registro de todo o passo-a-passo até a finalização da compra;

· Guarde **todos os e-mails** de confirmação do pedido, pagamento e qualquer outra comunicação que receba da loja.



USE DISPOSITIVOS SEGUROS

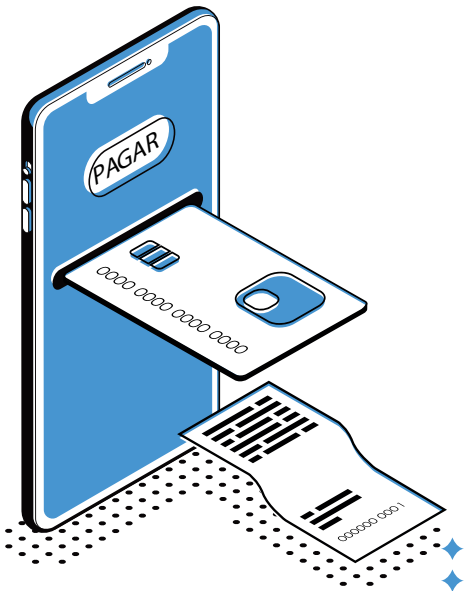
· Evite usar wi-fi público e computadores de terceiros para efetuar compras;

· Só realize as transações em smartphones e computadores seguros.

PREFIRA O CARTÃO VIRTUAL

· Se for utilizar o cartão de crédito, dê preferência para o uso do cartão virtual;

· A numeração temporária ou diferente do cartão físico e do código de segurança gerados pelos aplicativos dos bancos são válidos exclusivamente para uso on-line.



SE VOCÊ FOI VÍTIMA DE UM CRIME VIRTUAL, ENTRE EM CONTATO COM...

POLICIA CIVIL

Não deixe de ir a uma delegacia registrar o caso. É importante fazer uma print de tela que comprove o delito alegado, bem como a print da página do perfil do usuário que realizou a postagem falsa. Fique atento para que apareça a URL, que é o endereço da página.

PROCONRJ

Se na hora da compra de algum produto ou serviço você percebeu a tentativa de golpe e não foi vítima, denuncie pelo Whatsapp 21 98104-5445 para que outras pessoas recebam o alerta.

Se você foi vítima, abra uma reclamação pelo http://www.procononline.rj.gov.br/ ou pelo app Procon RJ