

# NOVA CARTILHA

GOIPE?  
TO  
FORA!



# SUMÁRIO

|                                                                  |    |
|------------------------------------------------------------------|----|
| Golpe do Bilhete Premiado                                        | 01 |
| Golpe do Falso Sequestro                                         | 02 |
| Golpe do Parente com Carro Quebrado                              | 03 |
| Golpe da Falsa Clonagem de Cartão Bancário                       | 04 |
| Golpe do Intermediador de Venda                                  | 05 |
| Golpe do "WhatsApp Hackeado"                                     | 06 |
| Golpe do Falso Boleto                                            | 08 |
| Golpe do Falso "Site"                                            | 09 |
| Golpe dos Falsos Fiscais                                         | 10 |
| Golpe do Falso Namorado                                          | 11 |
| Golpe da Troca de Cartão                                         | 12 |
| Golpes Decorrentes da Covid-19                                   | 13 |
| Golpe dos Falsos Agentes de Saúde                                | 14 |
| Golpe do Falso Leilão                                            | 15 |
| Golpe do Nudes - SEXTORSÃO                                       | 16 |
| Golpe do Falso Empréstimo                                        | 17 |
| Golpe do Falso Presente                                          | 18 |
| Golpe do Instagram Hackeado                                      | 19 |
| Golpe do Investimento Financeiro                                 | 20 |
| Golpe do Falso Link                                              | 21 |
| Golpe do Falso Pagamento por Meio de Pix                         | 22 |
| Golpe da Falsa Notificação Policial                              | 23 |
| Golpe da Falsa Herança                                           | 24 |
| Golpe do Acesso Remoto no Celular por Falso Funcionário de Banco | 25 |
| Golpe da Falsa Conta Cofre da Instituição Bancária               | 26 |
| Golpe dos Precatórios                                            | 27 |
| Golpe dos Valores de INSS                                        | 28 |
| Golpe do Cartão Travado no Caixa Eletrônico                      | 29 |
| Golpe da Devolução do Pix                                        | 30 |
| Golpe da Encomenda por Equívoco                                  | 31 |
| Patrocinadores                                                   | 32 |
| Orientações Gerais                                               | 36 |
| Dicas de Segurança                                               | 37 |





# Golpe do Bilhete Premiado



## Como o criminoso age:

O criminoso aborda a vítima com a desculpa de que está procurando uma loja/brechó ou uma casa lotérica. Surge outro criminoso na conversa (que pode falar com sotaque caipira) e diz que possui um bilhete premiado, um prêmio Jequití, uma Tele Sena, SP Cap, herança, etc., e que não pode receber todo o prêmio porque sua religião não permite ou porque precisa de duas testemunhas para recebê-lo.

Para que a vítima funcione como testemunha, o criminoso exige uma quantia em dinheiro para demonstrar boa-fé. Acreditando que um dos criminosos (que aparenta ser uma testemunha) deu dinheiro, a vítima vai até sua agência bancária e também saca dinheiro.

Ambos os criminosos dizem que precisam ir ao banheiro e desaparecem ou vão até o imóvel da vítima com a desculpa de pegar documentos pessoais ou comprovantes de residência. Quando a vítima entra em casa, os criminosos fogem com o dinheiro.

**Atenção!** Os criminosos estão bem vestidos, em um carro bom/novo e conversam bem.

**Orientação:** Diga que não está interessado e afaste-se. Se encontrar uma viatura policial, explique o ocorrido.

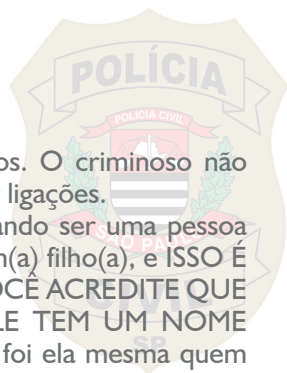


# Golpe do Falso Sequestro



## Como o criminoso age:

O criminoso liga aleatoriamente para muitos números. O criminoso não trabalha e, portanto, possui tempo de sobra para fazer ligações. A vítima atende, e o criminoso grita ao fundo, simulando ser uma pessoa sequestrada. A vítima, desesperada, fala o nome de um(a) filho(a), e ISSO É TUDO QUE O CRIMINOSO PRECISA PARA QUE VOCÊ ACREDITE QUE O SEQUESTRO É VERDADEIRO, POIS AGORA ELE TEM UM NOME FAMILIAR. A vítima, no desespero, não percebe que foi ela mesma quem forneceu o nome do(a) filho(a) e que não há sequestro algum.



## Orientações:

- Desligue o telefone.
- Caso se sinta mais seguro, escreva em um papel (enquanto estiver com o criminoso no telefone, pois ele não permite que a ligação seja desligada) o que está acontecendo. Leve o papel a um familiar, vizinho, padaria ou posto de gasolina e peça que liguem para o suposto sequestrado para verificar se está tudo bem. Assim, você ficará em paz e tranquilo.



# Golpe do Parente com o Carro Quebrado



## Como o criminoso age:

O criminoso liga, aleatoriamente, para muitos números. O criminoso não trabalha e, portanto, possui tempo de sobra para realizar ligações. Ele diz: "Oi, tio. Meu carro quebrou e preciso de ajuda." Na maioria das vezes, a vítima dá o nome de algum sobrinho, e o criminoso diz que acertou. Entretanto, se o tio/vítima não reconhece a voz, o criminoso diz: "Nossa, tio, você se esqueceu de mim? Não acredito!"

Constrangido, o tio/vítima acaba se sujeitando às solicitações. O criminoso pede que a vítima faça depósitos, transferências bancárias ou recargas para celulares, explicando que seriam formas de pagamento do conserto do veículo que estava quebrado na rodovia.

## Orientação

Desligue o telefone e ligue para o verdadeiro sobrinho que pensou estar conversando.



# Golpe da Falsa Clonagem de Cartão Bancário



## Como o criminoso age:

Um criminoso liga para a vítima e pergunta se ela emprestou o cartão a uma pessoa em outra cidade. Após a resposta negativa da vítima, ele pede que desligue o telefone e ligue para o 0800 no verso do cartão. O que a vítima não percebe é que a ligação não foi encerrada e o criminoso permaneceu na linha. Após a vítima discar o 0800 que consta no verso do cartão, o criminoso, que ainda está na linha, coloca uma gravação simulando ser da instituição bancária.

Acreditando estar falando com um funcionário da operadora do cartão, a vítima fornece seus dados pessoais, como nome, data de nascimento, RG, CPF, senha alfanumérica, telefone e endereço.

No final, o criminoso informa que um policial ou funcionário do banco passará para recolher o cartão clonado. Ele fornece um número de matrícula falso e orienta que o cartão seja entregue em um envelope endereçado ao banco ou à polícia. Com o cartão e as informações da vítima, os criminosos realizam saques, transferências bancárias, empréstimos, resgates de investimentos e compras, inclusive em maquininhas que possuem em seu poder.

## Orientação

- Se receber ligação de qualquer loja ou instituição financeira informando que seu cartão foi clonado, VÁ IMEDIATAMENTE À SUA AGÊNCIA BANCÁRIA E CONVERSE PESSOALMENTE COM O GERENTE ou consulte o aplicativo de seu banco. Fique alerta se utilizar site de bancos, pois os criminosos podem induzir a vítima a acessar sites falsos (e pedir atualização de dados), acreditando que realmente sejam de sua instituição bancária.
- Se tiver dificuldade para se locomover, peça ajuda a um familiar.
- JAMAIS ENTREGUE SEU CARTÃO A ESTRANHOS, mesmo que acredite que ele esteja cancelado ou cortado.
- Lembre-se: NEM O BANCO, TAMPOUCO A POLÍCIA NECESSITAM DE SEU CARTÃO BANCÁRIO PARA REALIZAR QUALQUER TIPO DE INVESTIGAÇÃO.

**Atenção:** Durante a pandemia do coronavírus, os criminosos alegavam que os bancos, para evitar contaminação de idosos, pediam que seus funcionários recolhessem os cartões bancários “clonados” em casa, É MENTIRA! Como já dito acima, nem o banco, tampouco a polícia precisam de seu cartão para investigar.



# Golpe do Intermediador de Venda



## Como o criminoso age:

O criminoso consegue o telefone da vítima em sites de vendas, como, por exemplo, "OLX" e "Webmotors". Afirmar para a vítima que tem interesse no bem oferecido e pede para que tire o anúncio da plataforma. Assim, o criminoso cria um novo anúncio com as fotos do bem da vítima, mas com valor bem abaixo do preço praticado no mercado, despertando o interesse de outras vítimas. Com a vítima interessada em vender o produto, o criminoso diz que comprará e pagará uma dívida que possui com seu cliente, sócio, amigo ou irmão, pedindo, portanto, silêncio no momento de apresentar o bem para outra vítima, prometendo algum lucro financeiro nesta negociação silenciosa. A vítima interessada em comprar, também é orientada a se manter em silêncio e, por isso, ganhará um desconto.

Com todo esse enredo e a enganação de que ambas as vítimas estão ganhando algo, o criminoso fornece uma ou algumas contas bancárias que não pertencem à vítima que está vendendo o bem. Com a transferência, ou até antes dela, o criminoso orienta as partes a irem até um cartório e preencherem o recibo do veículo, para dar mais veracidade ao golpe. Quando ambas as vítimas percebem o golpe, o recibo já foi preenchido, e todo o dinheiro da negociação foi parar na conta de um criminoso, que logo em seguida saca o montante, impedindo a recuperação do dinheiro.

## Orientação

Manter o maior diálogo possível entre vendedor e comprador. Sanar todas as dúvidas. **JAMAIS MANTER SILÊNCIO EM NEGOCIAÇÕES.** Só depositar ou transferir dinheiro para a conta bancária do titular do produto.





# Golpe do “WhatsApp Hackeado”



## Como o criminoso age:

O criminoso tem diversos meios de conseguir o número telefônico da vítima, mas tem sido observado que a maioria das vítimas acabara de efetuar anúncios em plataformas de comércio eletrônico. As vítimas recebem um torpedo "SMS" com um código de seis dígitos. Um criminoso se passa por funcionário desses aplicativos de vendas e solicita este código para ativar o anúncio. Na verdade, esse código é uma verificação do "WhatsApp". Assim que o criminoso digita o número de celular da vítima no "WhatsApp" dele, o código de verificação vai para o celular da vítima. O criminoso, então, utiliza o pretexto de que precisa do código para habilitar o anúncio, induzindo a vítima a fornecê-lo.

Após digitar os seis números fornecidos, o criminoso desvia o "WhatsApp" da vítima para o "WhatsApp" dele, e a vítima perde acesso ao aplicativo. O criminoso, então, conversa com os amigos e familiares da vítima pelo "WhatsApp", explica que está sem dinheiro, com a conta bancária travada ou cartão de crédito bloqueado, e solicita dinheiro emprestado, comprometendo-se a pagar o quanto antes. Os amigos/familiares da vítima acabam transferindo dinheiro para contas de laranjas/criminosos, que logo sacam ou transferem o valor, causando prejuízo às vítimas.

OBS.: O pretexto do criminoso para conseguir o código de seis dígitos varia, podendo ser para confirmar pesquisa do IBGE, validar descontos (voucher) em restaurantes/resort/hotéis, convites para shows, ativar anúncios de vendas, participar de programas de televisão, entre outros.

## Orientações

- Habilitar a “confirmação em duas etapas” no “WhatsApp”:
1. Clique em “Configurações / Ajustes”;
  2. Depois clique em “Conta”;
  3. Logo após, em “Confirmação em duas etapas”;

4. Habilite uma senha de seis dígitos numéricos.

- JAMAIS ENVIE PARA UM ESTRANHO O CÓDIGO, DE SEIS NÚMEROS, QUE CHEGA POR TORPEDO "SMS".

- Caso já tenha enviado o código para os criminosos e caído no golpe:

Envie um e-mail para: support@whatsapp.com;

2. No assunto, coloque: URGENTE WhatsApp Hackeado;

3. No corpo do e-mail, escreva: "Meu perfil foi hackeado e está sendo utilizado por criminosos, sem minha autorização. Estão solicitando dinheiro para os meus contatos. O perfil hackeado é o número +55 18 99XXX-XXXX. Solicito a desativação temporária e orientação para recuperação de meu perfil. Meu nome é (nome completo). Posso ser contatado pelo e-mail XXXXX@XXXXX. Desde já, muito obrigado."

Se o criminoso habilitar um número de celular diverso ao da vítima, mas utilizando sua foto no perfil e identidade, envie um e-mail para support@whatsapp.com solicitando a desativação definitiva da conta. Explique que um criminoso, com o número (exemplo: +55-18-99XXX-XXXX), está se passando por você e solicitando dinheiro aos seus contatos.

EM AMBOS OS CASOS, NO E-MAIL ENVIADO PARA O SUPORTE DO WHATSAPP, LEMBRAR DE COLOCAR O DDI DO BRASIL, +55, POIS QUEM IRÁ ANALISAR O PEDIDO ESTÁ FORA DO PAÍS. Para aqueles que receberem solicitações de dinheiro pelo "WhatsApp": Somente transfira ou deposite qualquer valor caso tenha confirmado, PESSOALMENTE, que o solicitante realmente é seu familiar ou conhecido. Não confie em ligações por vídeo para confirmar a veracidade do pedido, pois hoje em dia existe a Inteligência Artificial, que tornou possível essa ligação de maneira fraudulenta, imitando o rosto e a voz de seu familiar ou amigo, tampouco confie em perguntar datas importantes, pois hoje em dia temos o hábito de postar, em redes sociais, fotos com comentários em datas importantes e os criminosos possuem banco de dados.





# Golpe do Falso Boleto



## Como os criminosos agem:

Por meio de pesquisas que a vítima realiza na internet (criminosos estão impulsionando anúncios em sites de pesquisa), alguns criminosos virtuais conseguem identificar seus interesses e enviam boletos falsos por e-mail e whatsapp, como, por exemplo, boletos de contribuição à igreja, plano de internet, plano de saúde, financiamento, empréstimo, consórcio, etc. A vítima acredita que está pagando um boleto verdadeiro, mas no código de barras constam informações que direcionam o valor para a conta e o banco dos criminosos.

## Orientação

Caso receba um boleto inesperado, leve-o até o banco e converse com seu gerente. Antes de pagar qualquer boleto que tenha recebido por e-mail, whatsapp, caixa de correio, aplicativo, CONFIRA SE O BANCO QUE APARECE NA TELA DE PAGAMENTO É O MESMO QUE ESTÁ NO BOLETO. VERIFIQUE TAMBÉM O VALOR, A DATA DE VENCIMENTO, O BENEFICIÁRIO E DEMAIS DADOS.



# Golpe do Falso “Site”



## Como os criminosos agem:

Os criminosos criam sites falsos anunciando falsamente vendas de mercadorias, como eletrônicos e eletrodomésticos, hospedam o site no exterior visando dificultar sua retirada do ar. Agem intensamente durante a "Black Friday", mas atuam o ano inteiro. Usam o layout e endereço eletrônico de empresas famosas, alterando apenas o final do endereço, sendo assim, conseguem enganar as vítimas. Investem no impulsionamento de anúncios para aparecerem no topo dos resultados de busca e oferecem produtos com preços extremamente atrativos, aceitando diversas formas de pagamento e dando super descontos com pagamentos via PIX.

## Orientação

1. Verifique cuidadosamente todo o endereço eletrônico no navegador.
2. Pesquise a reputação da empresa antes de realizar a compra.
3. Desconfie de produtos com preços muito abaixo do praticado no mercado, mesmo durante promoções.
4. Lembre-se: *"Quando a esmola é demais, o santo desconfia!"*
5. Verificar sempre o beneficiário de pagamentos via boleto e Pix.
6. Prefira utilizar aplicativos de lojas conhecidas e confiáveis, mesmo que o preço seja ligeiramente maior.



# Golpe dos Falsos Fiscais



## Como o criminoso age:

Um criminoso contata vítimas com estabelecimentos comerciais, fingindo ser fiscal da Receita Federal ou Estadual. Alega que um lote de mercadorias foi apreendido e será leiloado, mas que pode ser vendido fora do leilão por um preço muito baixo. Após despertar o interesse da vítima, marca um encontro em locais renomados, como prefeituras ou hospitais. No local, fecham um suposto acordo e os criminosos exigem pagamento em espécie. Levam a vítima a mercados nos quais apresentam mercadorias como bebidas, pneus ou energéticos, alegando parceria com a Receita. Outra criminosa, se passando por gerente do mercado, reforça a história. Após receberem o dinheiro os criminosos fogem.

## Orientações:

- Fiscais da Receita Federal/Estadual não negociam fora da instituição.
- Mercadorias apreendidas só podem ser adquiridas oficialmente em leilões, com nota fiscal e dentro da lei.
- Desconfie de ofertas com valores muito abaixo do mercado.



# Golpe do Falso Namorado



## Como os criminosos agem:

Os criminosos procuram vítimas em sites de relacionamento e redes sociais. Após estabelecer contato, demonstram interesse amoroso e passam a se comunicar pelo WhatsApp. Fingem estar doentes e pedem dinheiro para tratamentos médicos. Em outra variação do crime, se passam por namorados estrangeiros, afirmando enviar presentes como joias, barra de ouro, dólares ou eletrônicos. Um cúmplice se apresenta como funcionário dos Correios ou alfândega, solicitando taxas para liberar o presente, pressionando emocionalmente a vítima. Os criminosos também têm convencido as vítimas a “comprar” as férias ou desligamento da empresa estrangeira para que possa vir até o Brasil conhece-las. Somente após realizar diversas transferências ou depósitos, a vítima percebe que era um golpe.

## Orientações:

1. Antes de confiar, encontre o(a) namorado(a) virtual pessoalmente, em locais públicos, para confirmar sua existência.
2. Nunca transfira dinheiro para namorados(as) virtuais.
3. Joias, barras de ouro e dólares não são enviados pelos Correios ou transportadoras. Se o remetente tem condições de enviar itens caros, também deve arcar com as taxas alfandegárias.
4. Para questões de saúde, oriente o(a) parceiro(a) a procurar o SUS, que cobre os custos necessários.
5. Férias e/ou desligamento de empresas não são custos arcados pelo trabalhador, mas pelo empregador.



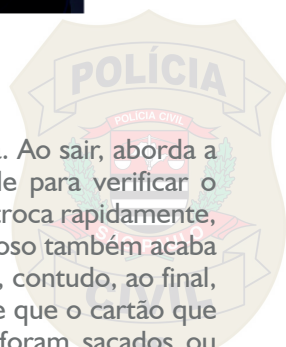


# Golpe da Troca de Cartão



## Como o criminoso age:

O criminoso observa a vítima dentro da agência bancária. Ao sair, aborda a vítima alegando um erro na transação financeira e pede para verificar o cartão. Quando a vítima entrega o cartão, o criminoso o troca rapidamente, diz que está tudo bem e vai embora. Por vezes, o criminoso também acaba por auxiliar a vítima ainda no interior da agência bancária, contudo, ao final, acaba por trocar os cartões. Mais tarde, a vítima percebe que o cartão que ficou com ela pertence a outra pessoa e que valores foram sacados ou transferidos de sua conta. Normalmente o criminoso está bem vestido, aparentando ser funcionário do banco, inclusive com crachá.



## Orientação:

Nunca entregue seu cartão bancário a terceiros ou pessoas desconhecidas.



# Golpes decorrentes da COVID-19



## Como os criminosos agem:

1. Envia mensagens oferecendo produtos como álcool em gel, máscaras, perfumes ou outros itens gratuitamente. Ao clicar em "CONTINUAR LENDO" ou no link, a vítima é direcionada para sites maliciosos, onde seus dados são capturados, ou ainda podem ter o celular bloqueado, com exigência de dinheiro para desbloqueio, bem como pode ser instalado aplicativo de acesso remoto ou espelhamento do celular.
2. Envia links para falsos cadastros do "Auxílio Emergencial" ou testes de COVID-19, solicitando dados bancários e pessoais, que são usados para acessar informações ou realizar transações fraudulentas.

## Orientação:

Não clique em links recebidos por WhatsApp, SMS ou e-mail de remetentes desconhecidos. Sites maliciosos podem capturar informações pessoais, bloquear celulares ou acessar dados bancários.

Apesar da contaminação da COVID-19 já estar sob controle, manteve o golpe aqui descrito, pois caso haja algo parecido com o que passamos em 2.020, os criminosos podem usar da mesma modalidade de golpe. Fique esperto!

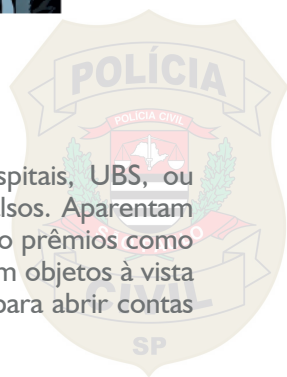


# Golpe dos Falsos Agentes de Saúde



## Como os criminosos agem:

Os criminosos se passam por agentes de saúde de hospitais, UBS, ou vigilância sanitária. Vestem jalecos, uniformes e crachás falsos. Aparentam simpatia, alegam estar realizando fiscalização ou oferecendo prêmios como massagens e dias de beleza. Enquanto estão no local, furtam objetos à vista e fotografam a vítima (selfie), usando as imagens e dados para abrir contas bancárias, realizar empréstimos ou aplicar outros golpes.



## Orientação:

Não permita a entrada de estranhos em sua casa, nem forneça dados pessoais ou permita que te fotografem. Esteja atento e evite facilitar a ação de criminosos.

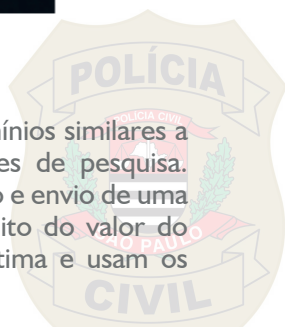


# Golpe do Falso Leilão



## Como os criminosos agem:

Criminosos criam sites falsos de leilões, com nomes e domínios similares a sites reais, promovendo anúncios que aparecem em sites de pesquisa. Oferecem preços baixos para atrair vítimas. Após o cadastro e envio de uma oferta, pedem cópias de documentos pessoais e o depósito do valor do lance. Assim que recebem o pagamento, bloqueiam a vítima e usam os documentos para novos golpes.



## Orientação:

- Verifique a reputação do site, por exemplo, no Reclame Aqui.
- Confirme o domínio do site (sites oficiais de leilões no Brasil possuem o sufixo “.com.br”).
- Realize pagamentos apenas para contas de pessoa jurídica do leiloeiro.
- Não pague valores antecipados como sinal ou frete.

## Caso tenha caído no golpe:

Registre a ocorrência policial. Preserve mensagens, e-mails e dados relacionados ao golpe. Capture imagens do site e dos anúncios fraudulentos para auxiliar a investigação.



# Golpe do Nudes - SEXTORSÃO



## Como o criminoso age:

O criminoso inicia contato com a vítima através de redes sociais como WhatsApp, Instagram ou Facebook, fingindo ser uma mulher. Ele envia uma foto íntima e pede que a vítima envie fotos similares. Após receber as fotos, o criminoso se passa pelo pai da suposta mulher ou por um delegado de polícia, alegando que a "filha" é menor de idade. Em seguida, ameaça registrar um boletim de ocorrência contra a vítima, exigindo transferências via PIX para evitar problemas. Caso se passe por delegado, o golpista cria um cenário falso com elementos policiais, como brasão da polícia, colete balístico e pastas com inscrições de "inquérito policial". O criminoso que se passa por genitor da menor ameaça enviar as fotos comprometedoras para familiares ou colegas de trabalho da vítima.

## Orientação:

Evite interagir com desconhecidos nas redes sociais e nunca envie fotos íntimas.

### Como a vítima deve proceder:

Se cair no golpe, não realize transferências. Caso tenha feito algum PIX, registre um boletim de ocorrência e apresente os comprovantes, chaves PIX e números de contato dos criminosos para auxiliar na investigação.



# Golpe do Falso Empréstimo



## Como os criminosos agem:

Por falhas de segurança nas instituições bancárias, criminosos têm tido êxito em realizar empréstimos em nome de vítimas. Após tais empréstimos que não foram solicitados pela vítima, os criminosos utilizam de artifícios como links fraudulentos ou aplicativos de acesso remoto para transferir o dinheiro do empréstimo da conta da vítima para a conta fraudulenta. Caso não consigam usar dos recursos acima descritos, eles também podem entrar em contato fingindo ser funcionário do banco, perguntando se a vítima solicitou um empréstimo e orientando-a a "devolver o dinheiro ao banco", quando na verdade o valor é transferido para contas de criminosos.

## Orientação:

Se um valor desconhecido aparecer em sua conta, procure imediatamente sua instituição bancária. Não transfira valores por PIX na intenção de devolver ao banco. Se a instituição colocou dinheiro em sua conta erroneamente, ela deve retirar este dinheiro sem que necessite de uma ação ativa da vítima. Apresente as conversas aos responsáveis pela instituição e solicite o resgate do dinheiro sem cobranças adicionais.





# Golpe do Falso Presente



## Como os criminosos agem:

Os criminosos descobrem a data de aniversário da vítima (por meio de rede social, venda de banco de dados e etc.) e se dirigem até a residência destas com supostos presentes como flores, chocolates ou perfumes, alegando que uma pessoa comprou para presentear, solicitou a entrega, mas que o frete não foi pago. Os criminosos exigem que o pagamento do frete seja realizado por meio do cartão de crédito, caso contrário o presente não será entregue. Sendo assim, os criminosos utilizam várias maquinações de pagamento e afirmam que o cartão não está passando, bem como colocam valores acima dos praticados por mototaxistas. Quando a vítima percebe, várias cobranças foram feitas em seu cartão.

## Orientação:

Se for solicitado o pagamento de frete, diga que irá retirar o presente diretamente na loja. Não forneça o cartão de crédito para pagamentos na porta de casa de compras que você não solicitou.

## Como a vítima deve proceder:

Caso tenha sido vítima, entre em contato com a central de atendimento do cartão de crédito e solicite o bloqueio do mesmo, bem como conteste as compras pleiteando a suspensão das mesmas. Também registre um boletim de ocorrência apresentando seu extrato bancário, bem como imagens das câmeras de vigilância, caso haja.



# Golpe do Instagram Hackeado



## Como os criminosos agem:

Os criminosos invadem a conta do Instagram da vítima e anunciam a venda de “produtos usados” ou oportunidades de investimento com retornos altos e rápidos. As vítimas que realizam pagamento para os criminosos acabam perdendo seu dinheiro.

## Orientação:

- Não clique em links de descontos, sorteios ou promoções duvidosas que cheguem no direct (aba de bate papo) de seu aplicativo.
- Habilite em seu perfil no Instagram a autenticação em dois fatores, preferencialmente usando aplicativos autenticadores.
- Evite comprar produtos anunciados em stories, especialmente se não for comum o contato (perfil de instagram) realizar vendas.

## Como a vítima deve proceder:

- Conta hackeada:

- 1.No aplicativo do Instagram, clique em "Esqueceu a senha".
- 2.Insira seu nome de usuário, e-mail ou número de celular e clique em "Encontrar a conta".
- 3.Caso o e-mail também tenha sido invadido, selecione "Não tem mais acesso a essas opções" e siga as instruções para recuperação da conta.
- 4.Grave um vídeo selfie em local iluminado, sem boné ou óculos, e forneça um e-mail nunca utilizado no Instagram.

- 5.Após a recuperação, ative a autenticação em duas etapas por meio de aplicativo autenticador.

- Pagamentos realizados:

Entre em contato com seu banco e solicite a Medida Especial de Devolução (MED), mecanismo do PIX que facilita a recuperação de valores em caso de fraude.

Como habilitar a autenticação em dois fatores:

- 1.Acesse as configurações do Instagram.
- 2.Clique em "Central de Contas" > "Senha e Segurança" > "Autenticação de dois fatores".
- 3.Escolha "App de autenticação" e siga as instruções para configurar o aplicativo sugerido (Microsoft Authenticator ou Google Authenticator).



# Golpe do Investimento Financeiro



## Como os criminosos agem:

Os criminosos, por meios virtuais, fazem a vítima acreditar que está realizando um grande investimento que pode ser acompanhado por um aplicativo. Eles ensinam a vítima a usar o aplicativo e pedem que ela compre ações de empresas ou criptomoedas por meio de transferências via PIX. A vítima não percebe que os pagamentos estão sendo feitos para pessoas físicas, e não para uma corretora de investimentos. Com um grande poder de persuasão, os criminosos convencem a vítima a fazer empréstimos para investir. A fraude é descoberta quando a vítima tenta resgatar o dinheiro e percebe que o aplicativo, na verdade, era apenas uma simulação e que os rendimentos exibidos nunca foram reais.

## Orientações:

- Invista apenas em instituições financeiras reconhecidas e pesquise sua reputação na internet. Sempre confira o beneficiário das transferências. Confie somente em corretoras de investimentos recomendadas e lembre-se: não existem rendimentos milagrosos, muito menos sem carência para resgate.

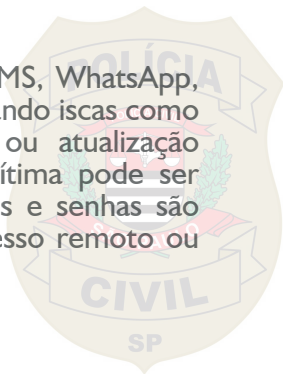


# Golpe do Falso Link



## Como os criminosos agem:

Os criminosos enviam links maliciosos por e-mail, SMS, WhatsApp, Facebook, Instagram, Telegram e outros meios, utilizando iscas como descontos, vouchers, prêmios, receitas culinárias ou atualização cadastral de bancos e lojas. Ao clicar no link, a vítima pode ser direcionada para um site falso, onde dados pessoais e senhas são solicitados, ou pode instalar vírus que permitem acesso remoto ou espionagem no dispositivo.



## Orientações:

Não clique em links enviados por remetentes desconhecidos, independentemente da oferta ou vantagem apresentada.

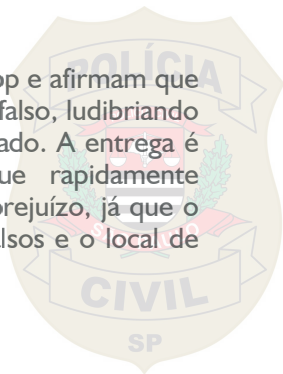


# Golpe do Falso Pagamento por Meio de PIX



## Como os criminosos agem:

Os criminosos realizam compras por telefone ou WhatsApp e afirmam que farão o pagamento via PIX. Eles enviam um comprovante falso, ludibriando o estabelecimento a acreditar que o pagamento foi efetuado. A entrega é feita em um endereço indicado pelos golpistas, que rapidamente desaparecem com a mercadoria. O comerciante fica no prejuízo, já que o pagamento nunca foi realizado, os dados utilizados são falsos e o local de entrega geralmente está desocupado.

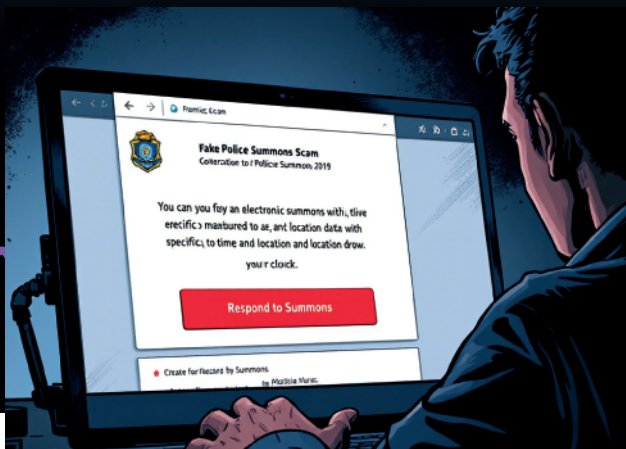


## Orientações:

Antes de liberar qualquer mercadoria, confirme o pagamento diretamente no aplicativo do banco. Não confie apenas no comprovante apresentado pelo cliente.

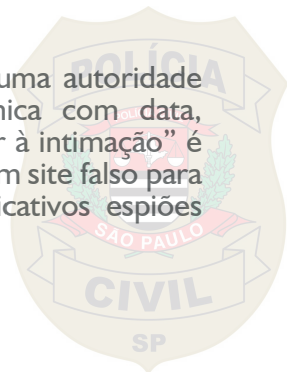


# Golpe da Falsa Notificação Policial



## Como os criminosos agem:

Os criminosos enviam um e-mail se passando por uma autoridade policial, informando sobre uma intimação eletrônica com data, horário e local. Ao final, um botão como “Responder à intimação” é oferecido. Ao clicar, a vítima pode ser direcionada a um site falso para coleta de dados pessoais ou pode ter vírus e aplicativos espíões instalados em seu dispositivo.



## Orientações:

Nunca clique em links ou botões sem verificar a autenticidade do remetente. No caso da Polícia Civil do Estado de São Paulo, por exemplo, o domínio correto do e-mail é @policiacivil.sp.gov.br. Notificações policiais verídicas podem ser enviadas por meios eletrônicos, mas nunca incluirão links clicáveis.



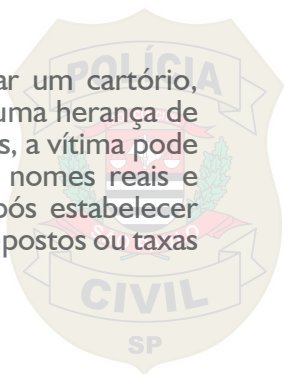


# Golpe da Falsa Herança



## Como os criminosos agem:

Criminosos entram em contato alegando representar um cartório, advogado ou instituição financeira. Informam que há uma herança de um parente distante ou que, por ausência de herdeiros, a vítima pode ser beneficiada devido ao sobrenome. Eles utilizam nomes reais e documentos falsificados para convencer a vítima. Após estabelecer contato, solicitam dados pessoais e o pagamento de impostos ou taxas legais.



## Orientações:

Desconfie de mensagens inesperadas e não interaja com desconhecidos. Nunca forneça informações pessoais, tampouco foto de documentos pessoais, não realize pagamentos a estranhos.



# Golpe do Acesso Remoto no Celular por Falso Funcionário de Banco



## Como os criminosos agem:

Os criminosos entram em contato informando que a conta bancária da vítima está sendo invadida e que procedimentos precisam ser realizados pelo aplicativo do banco. Como costumam agir fora do horário de funcionamento das agências, criam um cenário de urgência. Quando a vítima encontra dificuldade para seguir as instruções fraudulentas fornecidas pelos criminosos, que a vítima acredita que se trata de um funcionário do banco, os criminosos sugerem a instalação de um aplicativo de acesso remoto para que possam “ajudá-la”. Com isso, conseguem acessar o celular da vítima e realizam diversas transações fraudulentas.

## Orientações:

Nenhum banco exige a instalação de aplicativos de acesso remoto. Funcionários bancários possuem ferramentas para resolver problemas sem necessidade de intervenção no dispositivo do cliente. Em caso de dúvida, procure diretamente sua agência e fale com o gerente.

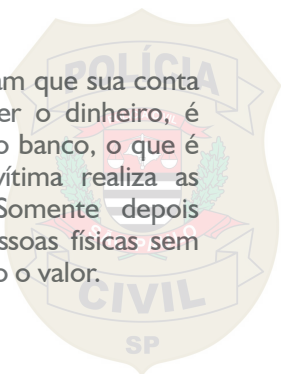


# Golpe da Falsa Conta Cofre da Instituição Bancária



## Como os criminosos agem:

Os criminosos entram em contato com a vítima e informam que sua conta bancária está sendo invadida. Alegam que, para proteger o dinheiro, é necessário transferi-lo para uma suposta "Conta Cofre" do banco, o que é uma fraude. Assustada e acreditando na história, a vítima realiza as transferências, incluindo investimentos e poupança. Somente depois percebe que enviou dinheiro via PIX para contas de pessoas físicas sem qualquer vínculo com a instituição bancária, perdendo todo o valor.

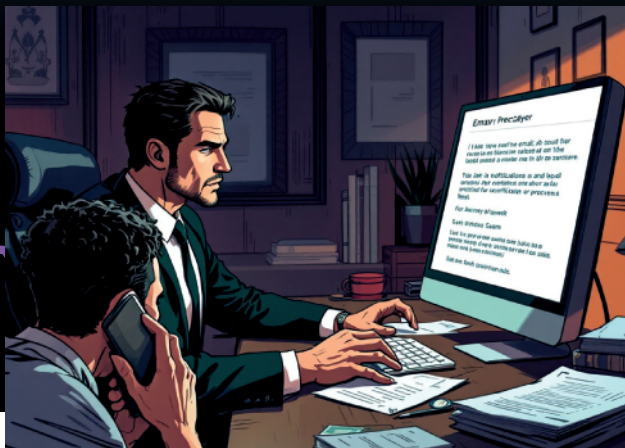


## Orientações:

Não existe "Conta Cofre" nas instituições bancárias. Os bancos possuem sistemas de segurança e equipes de detecção de fraudes que não exigem ações como essas dos correntistas. Proteja seus dados pessoais, cartões, senhas e nunca permita a instalação de aplicativos de acesso remoto em seu celular ou computador.

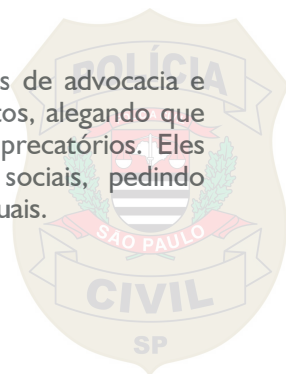


# Golpe dos Precatórios



## Como os criminosos agem:

Os criminosos se passam por funcionários de escritórios de advocacia e entram em contato com a vítima para solicitar pagamentos, alegando que são necessários para liberar um crédito relacionado a precatórios. Eles enviam mensagens por e-mail, WhatsApp ou redes sociais, pedindo transferências para custear certidões ou despesas processuais.



## Orientações:

Não responda a mensagens suspeitas. Procure o advogado responsável pelo caso ou informe-se diretamente no Fórum de sua cidade.

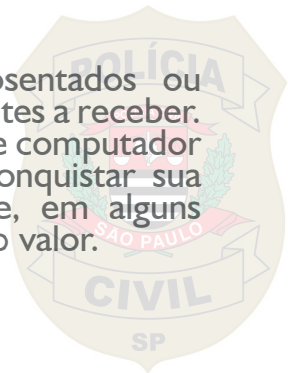


# Golpe dos Valores de INSS



## Como os criminosos agem:

Criminosos entram em contato com aposentados ou pensionistas, afirmando que há valores pendentes a receber. Para dar credibilidade, enviam fotos de telas de computador contendo dados pessoais da vítima. Após conquistar sua confiança, solicitam fotos de documentos e, em alguns casos, o pagamento de uma taxa para liberar o valor.



## Orientações:

Não forneça informações pessoais nem imagens de documentos. Criminosos podem usar essas informações para habilitar chips de celular, abrir contas bancárias e realizar empréstimos fraudulentos. Nunca realize pagamentos a estranhos que apresentem argumentos duvidosos ou vantajosos demais.

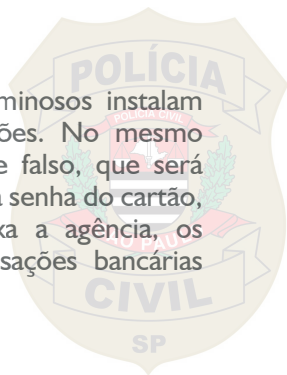


# Golpe do Cartão Travado no Caixa Eletrônico



## Como os criminosos agem:

Após o horário de funcionamento das agências, os criminosos instalam dispositivos nos caixas eletrônicos para travar os cartões. No mesmo terminal, deixam adesivos com um número de telefone falso, que será atendido por um comparsa. Este solicita dados pessoais e a senha do cartão, alegando que irá bloqueá-lo. Assim que a vítima deixa a agência, os criminosos recuperam o cartão preso e realizam transações bancárias utilizando as informações fornecidas.



## Orientações:

Antes de inserir o cartão, verifique se há dispositivos estranhos no terminal. Tenha anotado o número oficial de atendimento que consta no verso do cartão. Caso o cartão fique preso, entre em contato imediatamente com o banco por meio dos canais oficiais.



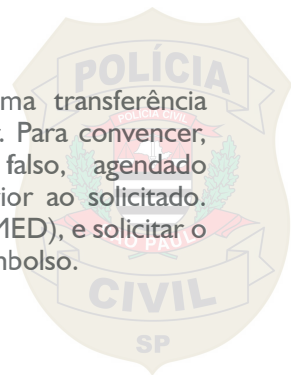


# Golpe da Devolução do PIX



## Como os criminosos agem:

O criminoso entra em contato alegando ter feito uma transferência equivocada para a vítima e solicita a devolução do valor. Para convencer, envia um comprovante de PIX, que pode ser falso, agendado (posteriormente cancelado) ou real, mas de valor inferior ao solicitado. Além disso, pode utilizar a *Medida Especial de Devolução* (MED), e solicitar o estornando do valor enviado à vítima após receber o reembolso.



## Orientações:

Verifique no aplicativo do banco se o valor realmente foi creditado em sua conta. Oriente o solicitante a procurar a instituição bancária para acionar a MED. Caso o banco indefira o pedido e a situação pareça legítima, considere realizar a devolução, com cautela.



# Golpe da encomenda por equívoco



## Como os criminosos agem:

Os criminosos enviam para a residência da vítima um pacote com embrulho perfeito, como se fosse realmente de uma empresa séria. Contudo, ao receber, a vítima percebe que o pacote não lhe pertence, que não pediu tal encomenda. E a orientação do criminoso é que se chegou com defeito, algum erro, ou se não lhe pertence que você deve entrar em determinado link, apontar sua câmera para um QR Code, ou então, contatar algum número de Whatsapp, e é neste instante que os criminosos conseguem instalar aplicativos de acesso remoto em seu celular e acessá-lo como se estivesse com o aparelho em mãos.

## Orientações:

Não receba encomendas que não estejam em seu nome ou de familiares, ou ainda, que esteja em seu nome, mas não foi solicitada por você. Não acessar nenhum QR Code para informar o recebimento equivocado, devolva no Correio ou galpões utilizados como depósitos de aplicativos de comércio eletrônico.

# PATROCINADOR

"Unir-se é um bom começo, manter a união é um progresso, e trabalhar em conjunto é a vitória". Henry Ford.

A partir da união das empresas abaixo foi possível tornar nosso sonho de informar a população uma realidade. Obrigada!"



Delegacia Seccional  
de Presidente Prudente





# PATROCINADOR

# PATROCINADOR



# PATROCINADOR



## O que é e como funciona o Mecanismo Especial de Devolução (MED):

O MED é um mecanismo exclusivo do PIX, criado para auxiliar possíveis vítimas de golpes e facilitar a devolução dos valores em duas situações específicas:

Confirmação de uso do PIX para aplicação de golpe;

Falha operacional nos sistemas das instituições envolvidas na transação.

Mas fique atento! O MED não se aplica em casos de:

Desacordo ou controvérsia comercial;

Erro na digitação dos dados do PIX (especialmente a chave do recebedor).

### Como solicitar a devolução:

Você deve registrar o pedido na sua instituição financeira em até 80 dias a partir da data da transação, nos casos de fraude, golpe ou falha operacional.

### Funciona assim:

Você registra a reclamação na sua instituição;

A instituição avalia o caso e, se enquadrado no MED, os recursos do recebedor são bloqueados;

O prazo para análise é de até 7 dias;

Se não for fraude, os recursos são desbloqueados para o recebedor;

Se confirmada a fraude, a devolução (total ou parcial) ocorre em até 96 horas.

Em casos de falha operacional (ex.: transação duplicada), a instituição analisa e, se comprovada a falha, o dinheiro é devolvido em até 24 horas.

# DICAS DE SEGURANÇA

- Em casos de irregularidades em sua conta, cartão ou invasão bancária, procure uma agência física e converse diretamente com seu gerente financeiro.
- Bancos não enviam funcionários para recolher cartões de crédito na residência de clientes e não solicitam cartas de contestação, senhas, dados pessoais ou instalação de aplicativos.
- Não realize pagamentos ou transferências sem antes falar pessoalmente com quem está solicitando. Fique atento a vídeos gerados por inteligência artificial.
- Nunca realize pagamentos se o beneficiário não for o legítimo proprietário do bem (por exemplo: o dono do veículo).
- Não entregue mercadorias antes de confirmar, diretamente no aplicativo do banco, se o pagamento foi efetivamente realizado. Existem comprovantes de PIX falsos.
- Não salvar senhas no bloco de notas do celular, pois caso o mesmo seja espelhado, acessado remotamente, furtado ou roubado os criminosos terão acesso a todas suas senhas.

## CUIDADOS COM DADOS PESSOAIS

Evite postar informações pessoais em redes sociais, como:

- Vínculos familiares (primo, irmão, marido, filho);
- Telefones (fixo ou celular);
- Endereço;
- Fotos de filhos com uniformes escolares;
- Informações sobre seu local de trabalho ou lugares frequentados (restaurantes, academias, entre outros);
- Fotos da família, especialmente de crianças.
- Datas especiais como nascimento de filho, casamento, entre outros.

Criminosos têm utilizado inteligência artificial para cometer fraudes. Não aceite solicitações de amizade de desconhecidos em redes sociais.

## APARÊNCIA DOS GOLPISTAS

Muitos criminosos envolvidos em estelionato apresentam boa aparência, falam corretamente, têm cabelo bem cortado e, geralmente, não utilizam armas, pois possuem um grande poder de persuasão. Esses golpes, frequentemente, são aplicados por meio de computadores ou outros dispositivos.

Lembre-se: “Quando a esmola é demais, o santo desconfia.” Em tempos de dificuldades financeiras, ninguém oferece dinheiro ou vantagens sem interesses ocultos.

# DICAS DE SEGURANÇA

## EM CASO DE SUSPEITA, PROCURE AJUDA.

Se desconfiar que está sendo alvo de golpistas, procure imediatamente:

- Delegacia de Polícia;
- Viatura Policial; ou
- Ligue para:
  - 190 - Polícia Militar
  - 197 - Polícia Civil

### AVISO

Esta cartilha foi elaborada para a informação gratuita de toda a população. Sua reprodução é permitida, desde que citadas as fontes. A venda ou comercialização deste material é proibida.

### DESENVOLVIDA POR:



Bárbara  
Camapum

 podbah.camapum



DC Marketing

 tarcisio\_dc



Operacionais  
GTTO

 operacionais GTTO  
 operacionais\_gtto

### APOIO:



Delegacia Seccional  
de Presidente Prudente