DISTRIBUIÇÃO GRATUITA
VENDA PROIBIDA

CARTILHA
GOLPE? TÔ FORA!

Conheça os principais golpes de estelionato praticados na atualidade. A informação ainda é a melhor forma de se proteger contra criminosos. **Fique ligado e compartilhe!**

Delegacia Seccional de Presidente Prudente

Operacionais GTTO
operacionais GTTO
operacionais_gtto

Bárbara Camapum
barbaracamapum

Duarte Coelho Marketing
tarcisio_dc

Emília Andrade

Márcio Henrique Oliveira

1ª Impressão

BANK
PAGAR
ONLINE
24/7
ECONOMIZE
50%

Delegacia Seccional de Presidente Prudente

Operacionais GTTO

operacionais GTTO
operacionais_gtto

Bárbara Camapum

barbaracamapum

Duarte Coelho Marketing

tarcisio_dc

Emília Andrade

Márcio Henrique Oliveira

ESTA CARTILHA É PARA MIM?

Esta cartilha foi desenvolvida com o objetivo de instruir a população quanto aos golpes que estão sendo praticados na atualidade.

É sabido que os criminosos sempre estão criando novos golpes, o que pode tornar esta cartilha obsoleta, mas lembre-se que os golpes são cíclicos, ou seja, os criminosos sempre voltam a utilizá-los, mudando pequenos detalhes.

Este projeto foi desenvolvido com muito carinho, objetivando que as pessoas não se tornem vítimas de estelionato. A linguagem utilizada é simples, para que atinja o maior número de pessoas.

Esperamos que tudo o que foi explicado possa auxiliar todas as pessoas. Repassem os conhecimentos contidos aqui a seus familiares, para se prevenirem dos golpistas.

Boa leitura!

Expediente:
Polícia Seccional de Presidente Prudente - SP.
Elaboração: Bárbara Camapum
Diagramação: Duarte Coelho Marketing
Revisão: Tarcísio Duarte Coelho
Créditos das Imagens: Freepik

Presidente Prudente - SP | 2020

SUMÁRIO:

Golpe do bilhete 03

Golpe do falso sequestro 04

Golpe do parente que o carro quebrou 05

Golpe do cartão bancário clonado 06

Golpe do intermediador de vendas 07

Golpe do WhatsApp clonado..... 08

Golpe do falso boleto 09

Golpe do falso site 10

Golpe dos falsos fiscais 11

Golpe do falso namorado 12

Golpe da troca de cartão 13

Golpe do **Coronavírus** 14

Orientações gerais 15

GOLPE DO BILHETE PREMIADO

Como o criminoso age:

O criminoso aborda a vítima com uma desculpa que está procurando uma loja ou uma casa lotérica. Surge um outro criminoso na conversa e diz que possui um bilhete premiado, um prêmio Jequiti, uma Tele Sena, SP CAP, herança etc.; e que não pode receber todo o prêmio, pois sua religião não permite ou ainda, que para receber o prêmio precisa de duas testemunhas.

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

Ambos os criminoso dizem que precisam ir ao banheiro e desaparece ou então, vai até a residência da vítima com a desculpa de pegar documentos ou comprovante de residência. Quando a vítima entra em casa os criminosos vão embora com o dinheiro.

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

Orientação: Fale que não está interessado e saia de perto. Se encontrar uma viatura policial, explique o ocorrido.

GOLPE DO FALSO SEQUESTRO

Como o criminoso age:

O criminoso liga de maneira aleatória para muitos números. Geralmente este criminoso está preso e possui tempo de sobra para efetuar ligações. A vítima atende e o criminoso grita ao fundo como se fosse uma pessoa sequestrada. A vítima desesperada fala o nome de um(a) filho(a) e 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 lhe traga mais segurança escreva em um papel o que está acontecendo e leve até um familiar, vizinho, padaria, posto de gasolina e peça para que liguem para o falso sequestrado, para saber se está tudo bem, pois assim a vítima irá se sentir em paz e tranquila.

GOLPE DO PARENTE COM CARRO QUEBRADO

Como o criminoso age:

O criminoso telefona de maneira aleatória para diversos números, em muitos casos este criminoso está preso e possui muito tempo disponível. O criminoso 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 a vítima acertou. Entretanto, se o tio/vítima não se recorda da voz, o criminoso diz: - Nossa, tio. Você se esqueceu de mim? Não acredito! O tio/vítima constrangido e acaba se sujeitando às solicitações. O criminoso pede para que a vítima faça depósitos, transferências bancárias ou ainda, recargas para celular.

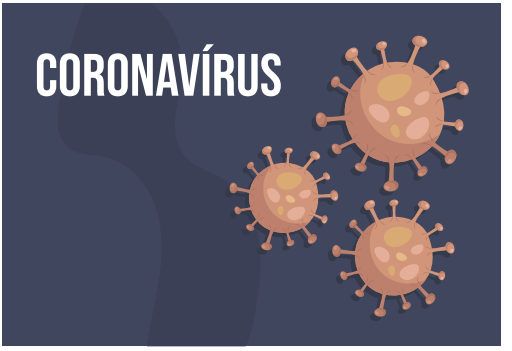
Orientação: Desligue o telefone e ligue para o verdadeiro sobrinho que pensou estar conversando.

GOLPE DA FALSA CLONAGEM DE CARTÃO BANCÁRIO

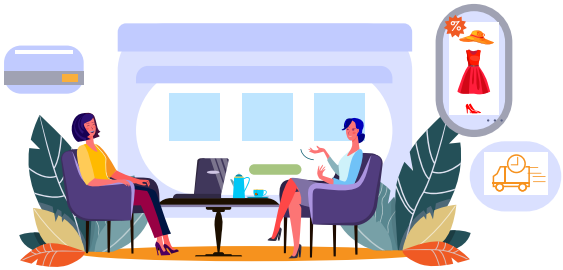
Como o criminoso age:
Um criminoso liga para a vítima e questiona se ela emprestou o cartão para uma determinada pessoa que está em outra cidade, sem ser a da vítima. Após resposta negativa da vítima, o criminoso pede para que ela desligue o telefone e ligue para o 0800 que consta no verso do cartão. O que a vítima não percebe, é que a ligação não foi encerrada e o criminoso continuou na linha telefônica. Após a vítima discar o 0800, o criminoso coloca uma gravação como se fosse uma instituição bancária. A vítima acreditando que está falando com uma funcionária da operadora do cartão, fornece seus dados pessoais como por exemplo, nome, data de nascimento, RG, CPF, senha alfanumérica, telefone e endereço.
Ao final, o criminoso diz que um policial ou funcionário do banco passará para coletar o cartão clonado, fornece o número de matrícula da pessoa que buscará. O criminoso informa para a vítima que o cartão já foi cancelado e que este deverá estar dentro de um envelope endereçado ao banco ou à polícia quando for entregue ao (falso) policial/-funcionário do banco. Com este cartão em mãos e todas as informações da vítima, o criminoso que recolheu o cartão realiza saques e transferências bancárias, compras em lojas físicas, bem como utiliza o cartão em maquininhas que estão em poder dos criminosos. Estas maquininhas são de lojas de todos os estados da Federação.

Orientações: Quando receber ligação de qualquer loja ou instituição financeira dizendo que seu cartão foi clonado e que estão realizando compras, VÁ IMEDIATAMENTE ATÉ SUA AGÊNCIA BANCÁRIA E CONVERSE, PESSOALMENTE, COM SEU GERENTE. No caso de dificuldade para se locomover, peça auxílio para um familiar. JAMAIS ENTREGUE seu CARTÃO a ESTRANHOS, mesmo que você acredite que ele esteja cancelado ou cortado. Saiba que nem o banco, tampouco a polícia precisam de seu cartão para investigar.

Atenção: Com a pandemia do CORONAVÍRUS, os criminosos estão dizendo que os bancos, para evitar contaminação de idosos, pedem que seus funcionários busquem o cartão bancário em casa. Isso é MENTIRA!



GOLPE DO INTERMEDIADOR DE VENDA



Como o criminoso age:

O criminoso consegue o telefone da vítima em "sites" de vendas, como por exemplo: "OLX", "Webmotors" etc. Afirma para a vítima que tem interesse no bem oferecido no aplicativo 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, o que desperta 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 e, portanto, pede 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, enganação de que ambas as vítimas estão ganhando um pouco, o criminoso fornece uma ou algumas contas bancárias diversas da conta da 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, tudo 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 todo o montante da conta, o que impede a recuperação do dinheiro.

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

GOLPE DO "*WHATSAPP* HACKEADO"

Como o criminoso age:

O criminoso tem diversos meios de conseguir o número telefônico da vítima, mas se tem observado que a maioria das vítimas tinham acabado de efetuar anúncio em plataformas como: "WebMotors" e "OLX". As vítimas recebem um torpedo de "SMS" no qual consta um código de seis dígitos. Um criminoso se passa por funcionário da "WebMotors", "OLX", Mercado Livre, bem como outros aplicativos de vendas, e solicita este código para ativar o anúncio; quando na verdade este código é uma verificação do "WhatsApp", ou seja, o criminoso digitou o número de celular da vítima no "WhatsApp" dele. Sendo assim, o código de verificação para habilitar o "WhatsApp" foi para o celular da vítima, por isso o criminoso se aproveita deste pretexto, de que necessita do código para habilitar o anúncio, induzindo a vítima a fornecê-lo. Assim que o criminoso digitar os seis números que a vítima forneceu, ele desvia o "WhatsApp" da vítima para o "WhatsApp" dele, e a vítima perde o acesso ao aplicativo. Com tal feito, o criminoso conversa com os amigos da vítima por "WhatsApp", explica que está sem dinheiro, com a conta bancária travada ou cartão de crédito bloqueado e solicita dinheiro emprestado, se comprometendo a pagar o quanto antes. Os amigos da vítima acabam por transferir dinheiro para a conta bancária de laranjas/criminosos, que logo sacam ou transferem todo o dinheiro, acabando assim, por se tornarem vítimas também. OBS.: O pretexto do criminoso para conseguir o código de seis dígitos que chega por "SMS" no celular da vítima sofre variações, podendo ser elas: confirmar pesquisa do IBGE, validar desconto em restaurante, convites para "shows", bem como para programa de televisão etc.

Orientações: (1) Habilitar a "confirmação em duas etapas"– no "WhatsApp" clicar em "Configurações / Ajustes", depois clicar em "Conta" e depois em "confirmação em duas etapas"; habilitar senha de seis dígitos numéricos. (2) Jamais enviar para qualquer pessoa o código de seis números que chega por torpedo "SMS". (3) Caso já tenha enviado o código e caído no golpe, envie um "e-mail" para "support@whatsapp.com" pedindo a desativação temporária de sua conta do "WhatsApp", explicando que seu número (exemplo: +55-18-99XXX-XXXX) foi "hackeado", e que alguém está se passando por você e solicitando dinheiro para os seus contatos. (4) Para aqueles que receberem solicitação de dinheiro por meio de "WhatsApp": somente transfira ou deposite qualquer valor caso tenha confirmado, pessoalmente, se o solicitante está realmente precisando de dinheiro. (5) Caso o criminoso habilite um NÚMERO DE CELULAR DIVERSO ao da vítima, mas utilizando de sua foto no perfil e de sua identidade: envie um e-mail para support@whatsapp.com pedindo a desativação da conta de WhatsApp, explicando que um criminoso com o número (exemplo: +55-18-99XXX-XXXX) está se passando por você e solicitando dinheiro aos seus contatos.

GOLPE DO FALSO BOLETO

Como o criminoso age:

Por meio de pesquisas que a vítima realiza em "sites" que acessa, alguns criminosos virtuais conseguem saber de seus interesses e assim enviam boletos falsos por "e-mail", como por exemplo, boletos de igreja, de Aparecida do Norte, do Divino Pai Eterno, do plano de "internet", do financiamento, do empréstimo, do 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.

Orientações: Caso chegue um boleto que você não está esperando, leve-o até o banco e converse com seu gerente. No momento de pagar o boleto confira se o banco que aparece na tela de pagamento é o mesmo que está no boleto, confira o valor, data de vencimento, beneficiado e demais dados.

GOLPE DO FALSO "SITE"

Como o criminoso age:

Os criminosos criam "sites" falsos de venda de mercadoria, como por exemplo, eletrônicos, eletrodomésticos etc. Agem de maneira extrema na "Black Friday", mas atuam em todas as épocas do ano. Usam endereços de empresas famosas, alterando só o final do endereço eletrônico, bem como usam o "layout" dos "sites" conhecidos, tudo para ludibriar a vítima de que se trata de "sites" verdadeiros.

Orientações: (1) Observar com cuidado todo o endereço eletrônico. (2) Pesquisar a reputação da empresa eletrônica em que pretende efetuar a compra. (3) Desconfiar de objetos que estejam à venda por preço muito abaixo daquele praticado no mercado. (4) Lembrando mais uma vez: QUANDO A ESMOLA É DEMAIS, O SANTO DESCONFIA!'

GOLPE DOS FALSO FISCAL

Como o criminoso age:

Um criminoso procura por vítimas que possuam comércio de qualquer ramo, liga para o estabelecimento e explica que é fiscal da Receita Federal/Estadual e que um lote de determinada mercadoria foi apreendida, que o lote irá a leilão, mas que se a vítima tiver interesse poderá vender fora do leilão por um valor bem abaixo do mercado. Após interesse da vítima, o criminoso marca um encontro na Prefeitura ou alguma outra instituição renomada, como por exemplo, Hospital do Câncer. No local, firmam acordo quanto ao valor da mercadoria, destaca-se que os criminosos exigem dinheiro em espécie. Os criminosos levam a vítima até um mercado e apresentam uma ilha de bebidas, energéticos, pneus etc. Explicam que o mercado é parceiro da Receita Federal/Estadual. Uma criminosa se apresenta como gerente do mercado e reafirma todo o alegado pelos criminosos. A vítima acredita na história e, portanto, entrega uma grande quantia em dinheiro para os criminosos. Estes pegam o carro e vão embora. Quando a vítima chega com o caminhão de frete para levar o lote de mercadoria, percebe que caiu em um golpe.

Orientações: Fiscais da Receita Federal/Estadual não tomam decisões independentes, fora da Instituição. Caso uma mercadoria vá a leilão, arremate no leilão, com nota fiscal e dentro do permitido pela Lei. Desconfie de mercadoria oferecida com valor abaixo do praticado pelo mercado.

GOLPE DO FALSO NAMORADO

Como o criminoso age:

Os criminosos procuram vítimas em sites de relacionamento, bem como em redes sociais. Após abordar a vítima virtualmente, demonstram interesse amoroso, acabam trocando contato de WhatsApp. As vítimas podem ser homens ou mulheres. O (a) namorado (a) virtual diz que está doente e que precisa de dinheiro para o tratamento. A vítima envolvida emocionalmente e com pena do (a) falso (a) namorado (a), acaba doando muito dinheiro, já que acredita na doença do (a) parceiro(a). Há também os casos em que os criminosos se passam por namorados (as) estrangeiros (as), iludem as vítimas e afirmam que estão enviando um presente, como por exemplo, flores, barra de ouro, joias, dólares, eletrônicos, perfume, bolsa, sapato etc. Um outro criminoso se passa por funcionário dos Correios/transportadoras ou da alfândega e solicita que um alto valor seja transferido para uma ou diversas contas bancárias, alegando que o presente ficou retido na alfândega ou Correios/transportadora. Com esta solicitação somada à pressão sentimental que o(a) falso(a) namorado(a) pratica, a vítima acaba cedendo e transfere ou deposita o dinheiro; posteriormente percebe que caiu em um golpe.

Orientações: (1) Encontrar o (a) namorado (a) que conheceu pela "internet" pessoalmente para saber se efetivamente existe. Destacamos, que o encontro seja em local público, pois ainda não se sabe quais as intenções do (a) namorado (a) virtual (2) Jamais transfira dinheiro para o (a) namorado (a) virtual. (3) Ninguém envia jóia, barra de ouro ou dólares pelos Correios ou transportadoras. E se o (a) namorado (a) possuir dinheiro a ponto de enviar ouro, joia ou dólares pelos Correios/transportadoras e correr o risco do extravio, oriente-o a também pagar pelas custas da alfândega e tributos da Receita Federal. (4) Quanto às solicitações para tratamento de saúde, há sistema público, como o SUS, que já realiza este papel, arcando com os devidos custos.

GOLPE DA TROCA DE CARTÃO

Como o criminoso age:

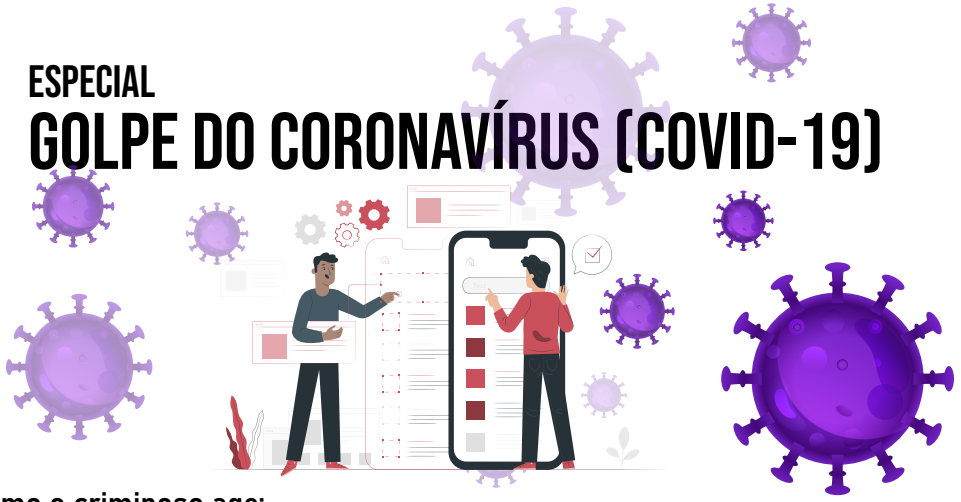
O criminoso observa a vítima no interior da agência bancária, quando ela sai, ele a aborda e explica que deu um erro em sua transação financeira e pede para ver o cartão da vítima.

Geralmente o criminoso está bem vestido, aparentando ser um funcionário do banco, inclusive utiliza crachá. Quando a vítima entrega o cartão ao criminoso, rapidamente ele troca o cartão, diz que não tem problema algum e vai embora. Quando a vítima percebe que o cartão que está com ela pertence a outra pessoa, vai até sua agência bancária ou consulta no aplicativo do banco e observa que valores foram sacados e transferidos de sua conta.

Orientação: Nunca entregue o cartão bancário para terceiros, ou seja, pessoas desconhecidas.

ESPECIAL

GOLPE DO CORONAVÍRUS (COVID-19)



Como o criminoso age:

(1) Os criminosos durante esta pandemia de Coronavírus (COVID-19) estão veiculando mensagens com a informação de distribuição gratuita de álcool em gel, cerveja, máscara de proteção, perfume, cafeteira e outros. Quando a vítima clica em CONTINUAR LENDO ou no LINK ela é direcionada para sites maliciosos que obterão seus dados, ou ainda acabam por bloquear o celular da vítima, oportunidade que os criminosos exigirão dinheiro para desbloqueá-lo.

(2) Os criminosos também estão veiculando mensagens com links que direcionam a vítima para uma espécie de cadastro do "Auxílio Emergencial", que é a ajuda do Governo Federal, quando a vítima clicar no link ela será remetida a uma ficha de cadastro, na qual os criminosos terão acesso a todas as informações que ela preencher e enviar, pois trata-se de um link falso.
Outro golpe que estão aplicando é o envio de mensagens com o link para fazer o teste de Coronavírus (COVID-19), o qual exige o nome do titular e dados do cartão bancário, e, por fim, o CPF da vítima. Após o envio os criminosos terão acesso aos dados bancários e pessoais da vítima.

Orientações: É muito importante que as pessoas não cliquem em "links" que chegam por mensagens de "WhatsApp", "SMS" e "e-mail", pois estes "links" vão direcionar a vítima para "sites" maliciosos que poderão obter informações pessoais, bem como bloquear o aparelho celular, oportunidade que os criminosos exigirão dinheiro para desbloqueá-lo; ou ainda, obterão dados de cartões bancários e pessoais.

ORIENTAÇÕES GERAIS

Muitos criminosos, que são autores de estelionato, não se vestem mal, falam corretamente, tem o cabelo bem cortado, geralmente não usam armas. Podem estar atrás de uma tela de computador. Sempre desconfiar de situações em que a ESMOLA É DEMAIS. Estamos em tempos difíceis financeiramente, ninguém está dando dinheiro facilmente.

Qualquer suspeita de que esteja sofrendo algum ataque de golpistas, procure uma delegacia de polícia, viatura policial ou ligue para:

190 - Polícia Militar
197 - Polícia Civil

Esta cartilha é para informação gratuita de toda a população. Sua reprodução é permitida, desde que citadas as fontes. Proibida a venda e comercialização.

Apoio:

Delegacia Seccional
de Presidente Prudente

Operacionais
GTTO
operacionais GTTO
operacionais_gtto

Bárbara
Camapum
barbaracamapum

Duarte Coelho
Marketing
tarcisio_dc

Emília
Andrade

Márcio Henrique
Oliveira