



# CUIDADO COM OS **GOLPES** NA INTERNET





# GOLPE DO AUXÍLIO EMERGENCIAL

**Como funciona o golpe:** Por meio de uma mensagem, o golpista ilude a pessoa afirmando que ela se enquadra no perfil para receber ajuda financeira do Governo, no valor que varia entre R\$600,00 e R\$1.200,00. Para ter acesso ao dinheiro, bastaria fazer um cadastro por meio do link informado na mensagem. **Aí que está a armadilha!** Nesse link, a vítima deve informar dados pessoais, como CPF, endereço, número da conta bancária e senha. O problema é que, a partir dessas informações, o cibercriminoso efetua diversos golpes, como abrir contas em bancos virtuais e solicitar cartões de crédito; ou abrir uma empresa fantasma em nome da vítima.

**Dica da PCRS:** Sempre desconfie de links enviados por *WhatsApp*, ainda mais quando estiverem associados a mensagens imediatistas, como "acesso somente nas próximas horas", "último dia para o saque", "o benefício se encerra hoje". Órgãos do Governo Federal não solicitam dados pessoais por meio de mensagens. Nunca preencha formulários com informações pessoais, principalmente CPF e dados bancários. Esses formulários geralmente chegam até as vítimas por mensagens no *WhatsApp*. Verifique junto ao site do Governo Federal a veracidade da informação. Se o benefício realmente existir, as regras para obtê-lo e o perfil de quem se enquadra estarão no site do Governo. Tenha um bom antivírus em seu celular e no seu computador. No celular é importante manter o sistema operacional do aparelho atualizado. Por fim, nunca compartilhe mensagens com links maliciosos, dos quais você não tem certeza da veracidade, confiabilidade e origem. Assim, você estará contribuindo para impedir esse tipo de golpe e garantir a segurança virtual de seus contatos.





# GOLPES EM SITES DE COMPRAS ONLINE:

**Como funciona o golpe:** A vítima faz um anúncio em algum site de compras on-line, expondo seu número de telefone para contato. De posse do número de telefone, o golpista, por mensagem ou ligação telefônica, engana a vítima dizendo que há a necessidade de atualização da conta/cadastro no site ou verificação do anúncio. Para validar a “atualização” ou “confirmação” do anúncio, o golpista solicita que a vítima lhe informe os 06 dígitos numéricos que ela receberá via SMS em seu celular. Todavia, estes números são, na verdade, o código de validação da conta do *WhatsApp*.

**Dica da PCRS:** Habilite a dupla verificação em seu *WhatsApp*. Não repasse códigos recebidos via SMS sem antes verificar a veracidade da solicitação feita pelo interlocutor;





## GOLPE DO FALSO SITE DE INTERNET:

**Como funciona o golpe:** Bandidos criam sites falsos de venda de mercadoria (eletrônicos, eletrodomésticos, etc.). Este golpe costuma ter maior incidência em datas comemorativas e promocionais, como por exemplo, a Black Friday. O golpista usa endereços de empresas famosas, alterando só o final do endereço eletrônico, bem como usam o layout dos sites conhecidos, tudo para ludibriar a vítima, fazendo-a pensar que se trata do site verdadeiro.

**Dica da PCRS:** Observe com cuidado todo o endereço eletrônico. Pesquise a reputação da empresa eletrônica em que pretende efetuar a compra. Desconfie de objetos que estejam à venda por preço muito abaixo daquele praticado no mercado.





# GOLPE DO INTERMEDIADOR DE VENDAS:

**Como funciona o golpe:** O golpista pega o telefone da vítima em sites de compras, e diz que tem interesse no objeto anunciado. Com o início da negociação, ele pede para que o anúncio seja retirado da plataforma. Com as informações do bem anunciado, o golpista cria um novo anúncio com as fotos da vítima, mas com um valor bem abaixo do preço praticado, o que desperta interesse de outras vítimas. Com a vítima interessada em vender o bem o golpista diz que comprará e pagará uma dívida que possui com algum cliente, sócio, amigo ou irmão, e, portanto pede silêncio no momento da apresentar o objeto para a segunda vítima, prometendo algum lucro financeiro nesta negociação silenciosa. Já a vítima interessada em comprar, também é orientada a se manter em silêncio e por isso ganhará um desconto. Com todo esse enredo, o golpista fornece uma ou algumas contas bancárias diversas da conta da vítima que está vendendo o bem, normalmente de terceiros “laranjas”. Com a transferência ou até antes dela, as vítimas ainda são orientadas a irem até um cartório e preencherem o recibo do veículo (quando a negociação é de carro), 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 bandido, que logo em seguida saca todo o montante da conta, o que impede a recuperação do dinheiro.

**Dica da PCRS:** Mantenha o diálogo aberto entre vendedor e comprador. Sempre procurar ver o objeto anunciado pessoalmente, em local público, movimentado e durante o dia. Conversar e reforçar a negociação pessoalmente. Na hora de fazer o pagamento, verificar o nome, CPF e número da conta do beneficiário.





## GOLPE DO DEPÓSITO COM ENVELOPE VAZIO:

**Como funciona o golpe:** Geralmente a vítima fez algum anúncio para venda de um determinado bem/objeto. O anúncio normalmente é feito pela internet em sites de compras ou por redes sociais. Após a negociação, o golpista faz o depósito do valor acertado em um caixa eletrônico ou lotérica, mas não deposita dentro do envelope o valor do bem/objeto. O golpista encaminha foto do comprovante de depósito e a vítima confirma o recebimento em consulta à sua conta pelo aplicativo do banco. Como a verificação bancária do depósito demora algumas horas, ou às vezes só é realizada no próximo dia útil, o valor fica aparecendo como depositado até que se verifique que o depósito não foi satisfeito. Até lá, a vítima já entregou o bem (normalmente o golpista manda um motorista por aplicativo buscar no mesmo dia do depósito o objeto).

**Dica da PCRS:** Quando realizada uma negociação pela internet, aguarde sempre a compensação do depósito bancário. É bom esperar o próximo dia útil para que haja a confirmação da entrada do dinheiro na conta.





# CLONAGEM DO WHATSAPP

**Como funciona o golpe:** Os golpistas têm diversos meios de conseguir o número da vítima, mas o mais usual é que seja retirado de anúncios em plataformas de sites de compras ou anúncios públicos (que abrangem não só os contatos da vítima) em redes sociais. As vítimas recebem um torpedo de SMS no qual consta um código de 6 dígitos. O golpista se passa por funcionário da plataforma de anúncio e solicita este código, alegando que isso é necessário para ativar o anúncio. Outras vezes alegam que houve duplicidade de anúncio, com valores diferentes. Para tal, solicitam a verificação da vítima com dados pessoais (nome completo, CPF, RG, endereço) e finalizando solicitam o código de 6 dígitos. Este código é uma verificação do *WhatsApp*, ou seja, o golpista digitou o número de celular da vítima no celular dele para ativar o *WhatsApp*. Este código de verificação para habilitar o *WhatsApp* foi enviado para o celular da vítima. É por este motivo que o bandido solicita o código, se aproveitando da vítima, de que este seria um passo necessário para habilitar o anúncio, induzindo a vítima a fornecê-lo. De posse desse código o golpista desvia o *WhatsApp* da vítima para o aplicativo instalado no celular dele, **e a vítima perde o acesso ao aplicativo**. Com tal feito, ele conversa com os amigos da vítima, **se fazendo passar por ela**, fala que está sem dinheiro, com algum problema na conta ou cartão de crédito bloqueado e solicita dinheiro emprestado, se comprometendo a pagar no dia seguinte. Os amigos da vítima, acreditando estarem falando com pessoa de sua confiança, acabam transferindo o dinheiro para a conta bancária informada, que normalmente é de algum laranja. Assim que a transferência é feita, eles também se tornam vítima do golpe.



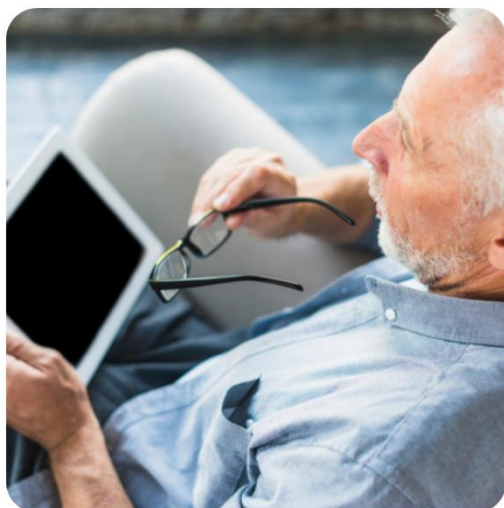
**Dica da PCRS:** É de suma importância habilitar a “confirmação em duas etapas” do *WhatsApp*. Para isso, clique em “Configurações/Ajustes”, depois clique em “Conta” e depois em “confirmação em duas etapas”; habilitar senha de 6 dígitos numéricos. Jamais enviar para qualquer pessoa o código de 6 números que chegar por torpedo SMS. Caso já tenha enviado o código e caído no golpe, enviar e-mail para [support@whatsapp.com](mailto:support@whatsapp.com) pedindo a desativação temporária de sua conta do *WhatsApp*, explicando o que ocorreu, bem como o seu número de *WhatsApp* (exemplo: +55-51-9XXXX-XXXX); Posteriormente, após receber o e-mail do *WhatsApp* no prazo de 30 dias, configure-o com o seu número de celular. Caso você receba uma mensagem de algum contato seu solicitando empréstimo de dinheiro ou depósito de algum valor em uma determinada conta, verifique com seu amigo a veracidade desta solicitação. E, caso seja verdade, antes de qualquer confirmação de depósito, verifique o destinatário (nome, CPF, agência bancária).



## GOLPE DO BILHETE PREMIADO:

**Como funciona o golpe:** A vítima (muitas vezes idosa) é abordada por uma pessoa humilde, que pede algumas informações, dizendo ter um bilhete de loteria premiado. O golpista, suposto ganhador da loteria, alega ter medo de ser enganado na hora de resgatar o prêmio ou que não teria os documentos necessários para sacar o prêmio, ou ainda que tem ações na justiça que o impediriam de receber o prêmio. Há vezes ainda em que o golpista alega motivos religiosos para não aceitar a premiação. Em seguida entra em cena o segundo golpista, um sujeito mais bem arrumado, que alega ter ouvido toda a conversa. Às vezes o primeiro golpista também aborda o seu comparsa, como se quisesse tirar alguma dúvida. Este segundo sujeito simula falar com alguém da Caixa Econômica Federal para confirmar a veracidade do prêmio. Nesse ponto, o golpista bem vestido propõe que a vítima fique com o bilhete e em contrapartida, repasse algum valor para o suposto ganhador do prêmio. Geralmente eles acompanham a vítima até uma agência bancária para fazer o saque do dinheiro, ou transferência “como garantia de que o humilde suposto ganhador não seja enganado”, e então entregam o bilhete premiado.

**Dica da PCRS:** Não existe ganho de dinheiro fácil, ainda mais em abordagens na rua por desconhecidos. Desconfie sempre. Caso alguém peça ajuda em alguma situação semelhante, diga que não pode ajudar e procure uma Delegacia de Polícia mais próxima para informar o fato.







## GOLPE DO FALSO SEQUESTRO:

**Como funciona o golpe:** O golpista liga de maneira aleatória para diversos números. Geralmente ele está preso e possui tempo de sobra para efetuar ligações. A vítima atende e o bandido grita no fundo, como se fosse uma pessoa “sequestrada”. A vítima desesperada fala o nome de um filho, sobrinho, alguém próximo. Com isso, o bandido consegue a informação que ele queria para fazer a vítima acreditar que se trata de um sequestro de verdade. No desespero, a vítima não percebe que foi ela mesma quem forneceu o nome do sequestrado, e às vezes, com o nervosismo, não percebe a diferença na voz. Neste momento o golpista pede que a vítima não desligue, que ela fique na linha até que alguém faça a transferência de um determinado valor para a conta de algum “laranja”.

**Dica da PCRS:** Desligue o telefone e faça contato com o suposto familiar que teria sido sequestrado. Caso tenha receio de desligar, acreditando ser verdadeiro o sequestro, peça para alguém próximo (um familiar ou vizinho) que faça contato com a suposta vítima do sequestro para saber se está tudo bem.





# GOLPE DO CARTÃO DE CRÉDITO CLONADO:

**Como funciona o golpe:** O golpista faz contato com a vítima se apresentando como alguém do cartão de crédito alegando que houve uma compra duvidosa no cartão da vítima e solicita que esta confirme ou não a compra. Como a vítima não reconhece esta compra, o golpista solicita que a vítima ligue para o 0800 que consta no verso do cartão para solicitar o cancelamento da compra e bloqueio do cartão. Neste momento, a vítima não percebe que o golpista continuou na ligação. Após “dispar” para o 0800, o golpista coloca uma gravação como se fosse do banco. Acreditando que está falando com uma pessoa da operadora do cartão, acaba fornecendo seus dados pessoais (nome completo, RG, CPF, data de nascimento e endereço para onde é encaminhada a fatura) e do cartão de crédito (número do cartão, nome como consta no cartão, data de vencimento da fatura, data de validade do cartão e código verificador – aquele de 3 dígitos no verso do cartão e senha). Depois de obter estas informações, o suposto atendente do cartão informa que enviará uma pessoa (funcionário do banco ou motoboy que trabalhe para o banco) para recolher o cartão clonado. Com o cartão em mãos e todos os dados pessoais da vítima, os golpistas fazem compras em diversas lojas físicas ou sites.

**Dica da PCR:** Caso você receba alguma ligação de qualquer loja, instituição financeira ou administradora de cartão de crédito, dizendo que seu cartão foi clonado, ou querendo que você confirme alguma compra que você não tenha feito, **procure a sua agência bancária** ou faça contato com o seu gerente de conta. Jamais entregue o seu cartão a alguém. **Nenhuma Instituição Financeira ou administradora de cartões de crédito envia pessoas nas residências dos clientes para recolher cartões clonados.**





# GOLPE DA TROCA DE CARTÃO:

**Como funciona o golpe:** A vítima, após ser observada inserindo os dados do cartão no caixa eletrônico por um dos golpistas, é abordada ao sair da agência bancária por pessoa que se apresenta como funcionário do banco. O golpista normalmente está bem vestido e apresenta um “crachá” do banco. Esta pessoa alega que houve algum problema na transação efetuada ou na máquina e solicita que a vítima retorne ao caixa eletrônico para verificarem a transação. Neste momento ele “auxilia” a vítima e rapidamente efetua a troca do cartão. Às vezes o golpista solicita apenas para verificar o cartão e neste momento efetua a troca.

**Dica da PCRS:** Nunca entregue seu cartão a terceiros. Caso precise de ajuda na agência bancária, procure sempre o funcionário da Instituição Financeira e mesmo assim, não entregue seu cartão. Escute as orientações e faça o procedimento. Caso não tenha muito conhecimento para operar a máquina, peça para que alguém de sua confiança o acompanhe até o banco.

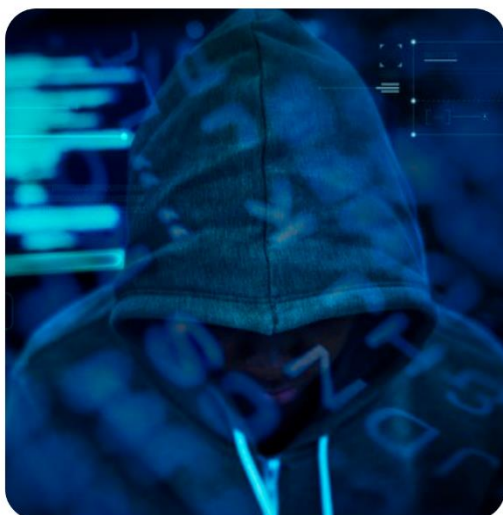




## GOLPE DO BOLETO FALSO:

**Como funciona o golpe:** Em tempos de pandemia, em razão do isolamento, muitas pessoas estão fazendo compras pela internet, redes sociais e até mesmo *WhatsApp*. Muitas vezes a vítima não está com acesso seguro aos sites visitados, seja pelo computador, seja pelo celular. Diversas são as formas de manipular a vítima neste momento. Pode ser por uma falsa página de alguma loja ou falso contato pelo *WhatsApp* para venda direta. Neste momento é emitido o boleto bancário para pagamento da compra efetuada. Este boleto possui cabeçalho e imagens aparentemente da loja/empresa em que a vítima estava negociando. O golpe pode ser realizado tanto com a manipulação do código de barras do documento ou com a criação de páginas falsas que oferecem o download da “fatura”. Neste momento o valor transferido/pago vai para a conta bancária do golpista ou de um “laranja”.

**Dica da PCRS:** Verifique sempre os dados do destinatário do boleto emitido. Antes de confirmar a transação ou pagamento, verifique se os dados do beneficiário conferem com os dados da loja/empresa. Caso queira emitir uma 2ª via de algum boleto, procure o site oficial do credor e verifique os dados do boleto emitido.





# GOLPE DO FALSO EMPRÉSTIMO:

**Como funciona o golpe:** Os golpistas fazem anúncios em sites, redes sociais ou até mesmo ofertas pelo *WhatsApp*. A oferta é bem tentadora: crédito fácil e rápido, juros mais baixos do que aqueles operados por Instituições Financeiras, possibilidade de pagar em diversas parcelas, sem consulta ao SPC/Serasa, e, caso a vítima esteja negativada, não impediria a concessão do crédito. Onde entra o golpe? Eles alegam que para que o crédito seja liberado para a vítima, é necessário que ela pague uma taxa! Os golpistas usam diversas alegações, seja taxa de abertura de crédito, taxa exigida pelo Banco Central, seguro de crédito, e por aí vai.

**Dica da PCRS:** Este golpe é facilmente identificado com a exigência de um depósito antecipado para a liberação do crédito. Lembre-se: Instituições Bancárias e Financeiras não solicitam depósito prévio. Você toma o dinheiro antes e paga depois. Não confie em ganhos fáceis e promessas extremamente vantajosas. Ainda mais se você não procurou uma Instituição Financeira, vinculada ao Banco Central. Desconfie sempre quando esta oferta “bate à sua porta”. Procure sempre pesquisar o nome da Instituição na internet, no “reclame aqui” e “Procon” antes da realização de qualquer contrato. Mesmo em tempos de pandemia, opte por fazer algum financiamento presencialmente no Banco ou Financeira. Caso você não entenda muito dos trâmites, solicite ajuda de uma pessoa de sua confiança.





## GOLPE DA TROCA DE FOTOS ÍNTIMAS:

**Como funciona o golpe:** Os golpistas utilizam as redes sociais para enganar suas vítimas. As vítimas podem ser homens ou mulheres, mas mais usualmente são homens, maiores de idade, e muitas vezes casados. O golpista utiliza um perfil falso, muitas vezes com a foto de uma jovem bonita e atraente. Eles começam uma amizade e logo o golpista, seja uma “jovem moça” ou um “rapaz atraente”, envia fotos íntimas suas e pede para que a vítima faça o mesmo. De posse dessas fotos íntimas da vítima, outro golpista entra em cena: o suposto pai ou padrasto da(o) jovem, alegando que este último é menor de idade e que a vítima estaria praticando o crime de pedofilia pela internet. Para que o pai/padrasto não leve o caso para a Polícia, ou não conte tudo para a esposa/marido da vítima, exige que seja paga uma quantia em dinheiro. Algumas vezes, os golpistas se fazem passar por policiais civis, alegando que as fotos já fazem parte de um Inquérito Policial e solicitam o depósito para que “a investigação seja arquivada”.

**Dica da PCRS:** Não troque, nem compartilhe fotos íntimas pela internet. Lembre-se: depois que a foto ou vídeo foi compartilhado, ele pode circular por milhares de pessoas. Desconfie de solicitações de amizade de pessoas que você não conhece. E o mais importante: Pedofilia é crime! Se a pessoa que você está fazendo uma nova amizade aparenta ser menor de idade, todo o cuidado é necessário!

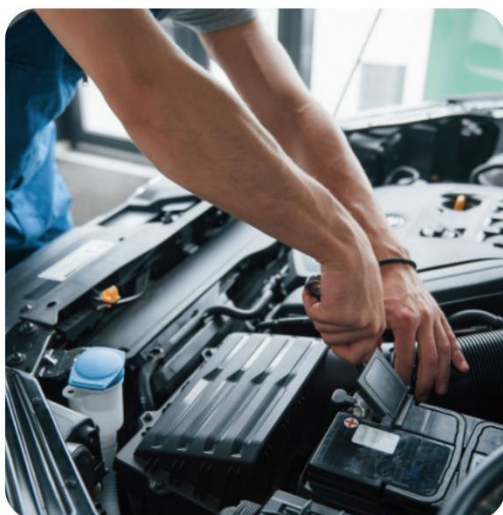




## GOLPE DO PARENTE QUE QUEBROU O CARRO:

**Como funciona o golpe:** O golpista liga aleatoriamente para as vítimas. Dependendo de quem atende for homem ou mulher, ele logo fala: “oi tio/tia, sabe quem está falando?” Caso a vítima diga um nome, achando ser algum sobrinho ou parente distante, já deu para o golpista o que ele queria. Algumas vezes a vítima fala que não se lembra e o golpista usa do artifício “nossa, não lembra mais de mim”. A vítima, constrangida, acaba continuando o diálogo e se sujeitando ao que o golpista fala. Com isso, ele conta uma história que seu carro quebrou e que precisa de ajuda, solicitando que a vítima faça uma transferência para determinada conta (seja do mecânico, da ferragem, ou da borracharia para pagar o conserto do carro).

**Dica da PCRS:** Não faça transferências ou dê dinheiro para terceiros. Deligue o telefone e faça contato com o familiar que você achava estar falando. Caso a pessoa esteja realmente em apuros, você ainda poderá ajudá-lo.





# GOLPE DO BOOK FOTOGRÁFICO:

**Como funciona o golpe:** Geralmente as vítimas aqui abordadas são idosas. Os golpistas abordam os mais idosos com a promessa de brindes, maquiagens e fotos gratuitas. Assim, após serem persuadidas, as vítimas aceitam fazer as fotos nos pequenos estúdios. Depois de uma produção de maquiagem, trocas de roupas e diversas fotos vem a surpresa: na saída as vítimas são constrangidas a pagar pelas fotos com valores bem altos.

**Dica da PCRS:** Não aceite propostas de abordagens na rua. Se você está interessada em fazer um book fotográfico, procure uma empresa séria e pesquise sobre a reputação desta na internet. Desconfie sempre!







## DICAS FINAIS DA PCRS:

1. Não forneça seus dados pessoais (como nome completo, CPF, RG, endereço, número da conta bancária e senha) para estranhos, em ligações telefônicas, mensagens SMS ou *WhatsApp*;
2. Desconfie sempre de ofertas de produtos com preços abaixo dos praticados em mercado;
3. Não converse com estranhos na rua, tão pouco aceite propostas que pareçam ser muito boas e que lhe trariam alguma espécie de “vantagem”;
4. Saiba que a aparência engana! Estelionatários falam bem, estão normalmente bem vestidos e facilmente persuadem as vítimas. Tome estes cuidados para não se tornar uma.
5. Não troque fotos nem vídeos íntimos pela internet/rede social. Lembre-se: pedofilia é crime.
6. Em caso de dúvida, procure sempre alguém de sua confiança e peça ajuda.
7. Se você sabe de alguém que pode estar praticando algum destes golpes, denuncie pelo 197, *WhatsApp* da Polícia Civil (51)98444-0606 ou procure a Delegacia de Polícia mais próxima.
8. Caso você tenha sido vítima de algum destes golpes, procure a Polícia Civil. Em tempos de pandemia, você pode registrar a ocorrência pela Delegacia Online:  
[www.delegaciaonline.rs.gov.br](http://www.delegaciaonline.rs.gov.br)

