POLÍCIA CIVIL RS

CUIDADO COM OS GOLPES NA INTERNET

GOLPE DO PAGAMENTO POR APROXIMAÇÃO:

COMO FUNCIONA O GOLPE:

Neste golpe, os criminosos entram em contato com lojistas e se passam por funcionários de empresas responsáveis pelas maquininhas de cartões. Eles utilizam como argumento a realização de uma suposta manutenção e solicitam acesso ao computador onde fica o sistema do aparelho. Quando os lojistas clicam no link introduzido na máquina pelos golpistas, é instalado um vírus que dá acesso remoto à maquininha. A partir da instalação desse malware, o equipamento passa a detectar e a impedir a cobrança por aproximação, exibindo uma mensagem falsa de erro, o que obriga o consumidor a inserir o cartão físico no aparelho. Com isso, a vítima tem dados capturados e o cartão pode ser clonado.

DICA DA PCRS:

- Em caso de erro, verifique com o lojista a possibilidade de fazer o pagamento por aproximação em outra máquina. Caso não seja possível ou apareça novamente a mensagem de erro, procure outra solução, como pagamento em dinheiro ou por pix. Evite inserir o cartão físico no aparelho.

- Esteja sempre atento à fatura do cartão. Caso perceba algum gasto indevido, entre em contato imediatamente com sua instituição financeira e registre boletim de ocorrência.

- Lojistas que utilizam máquina de cartão devem estar atentos aos pedidos de verificação ou manutenção das maquininhas, sobretudo se for necessária a instalação de algum software. É aconselhável fazer contato com a empresa do cartão para verificar se os procedimentos estão corretos.

GOLPE DO AUXÍLIO EMERGÊNCIAL:

COMO FUNCIONA O Ggolpe:

Os golpistas entram em contato com as possíveis vítimas por meio de mensagem no celular, via SMS ou WhatsApp. No contato, eles afirmam que a pessoa se enquadra no perfil para receber ajuda financeira do governo, podendo ganhar valores que vão de R$600 a R$1,2 mil. Para ter acesso a esse suposto benefício, os criminosos orientam a vítima a clicar em um link enviado no corpo da mensagem. Nesse link, a pessoa deve informar dados pessoais, como CPF, endereço, número da conta bancária e senha. Na posse dessas informações, os criminosos, então, passam a aplicar diversos golpes com o nome da vítima, como abertura de contas em bancos digitais, abertura de empresas fantasmas ou solicitação de cartões de crédito, por exemplo.

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" ou expressões semelhantes.

- Órgãos do Governo Federal não requisitam dados pessoais por meio de mensagens, por isso, esteja atento a solicitações desse tipo.

- Nunca preencha formulários com informações pessoais, principalmente CPF e dados bancários.

- Em caso de dúvida, 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 disponíveis no site do governo.

- Tenha um bom antivírus em seu celular e no seu computador. No celular, também é importante manter o sistema operacional do aparelho atualizado.

- Nunca compartilhe mensagens com links maliciosos ou dos quais você não tem certeza da veracidade, confiabilidade e origem. Assim, você contribuirá para impedir esse tipo de golpe e garantir a segurança virtual de seus contatos.

GOLPE EM SITE DE COMPRAS ONLINE:

COMO FUNCIONA O GOLPE:

Este golpe tem metodologia semelhante ao golpe da clonagem do Whatsapp. O alvo dos criminosos são pessoas que fizeram algum tipo de anúncio em site de compras, expondo seu número de telefone para contato. De posse do número, o golpista engana a vítima, por mensagem ou ligação telefônica, dizendo que há a necessidade de atualização da conta/cadastro no site ou de verificação do anúncio. Para realizar essa suposta validação, o criminoso solicita que a pessoa lhe informe os 06 dígitos numéricos que ela receberá via SMS em seu celular. Esses números, no entanto, são o código de validação da conta do WhatsApp do usuário. Uma vez que obtêm esses dados, os golpistas passam a ter acesso à conta do aplicativo de mensagens da vítima, por meio da qual aplicam diversos outros golpes.

DICA DA PCRS:

- Habilite a verificação em duas etapas em seu WhatsApp. Essa opção normalmente fica disponível no menu do aplicativo, dentro da opção “Conta”.

- Não repasse a terceiros os códigos recebidos via SMS sem antes verificar a veracidade da solicitação.

GOLPE DO INTERMEDIADOR DE VENDAS:

COMO FUNCIONA O Ggolpe:

Os criminosos fazem uma intermediação não autorizada de um produto para enganar o verdadeiro vendedor e o comprador. Para isso, localizam a vítima em sites de compras e fazem contato manifestando interesse em algum objeto anunciado por ela, geralmente veículos semi-novos. Após iniciada a negociação, eles solicitam ao vendedor que o anúncio do item seja retirado da plataforma. A partir daí, os golpistas criam um anúncio falso, com as fotos do produto originalmente anunciado pela vítima, mas com um valor bem abaixo do preço praticado, o que desperta o interesse de outros compradores.

Quando um comprador entra em contato através deste anúncio falso, o golpista diz que a venda do bem resolverá uma dívida com terceiros, geralmente parentes, funcionários, sócios ou até amigos e, na sequência, pede silêncio sobre a transação e sobre o valor combinado. Dessa forma, gera confiança, ao explicar a suposta razão do preço abaixo do mercado.

No caso da compra tratar-se de um veículo, registra-se que sempre é importante olhar o carro pessoalmente antes de fechar negócio. Assim, o fraudador aguarda até que o comprador demonstre essa vontade. Neste momento, ocorre a parte mais mirabolante do golpe do falso intermediário: o criminoso faz as duas vítimas se encontrarem, sem saber que estão conversando com outra pessoa, e não com o dono do anúncio. Para isso, o golpista marca com ambas as vítimas um dia, local e horário para ver o carro. Para o vendedor, o criminoso diz que um parente, funcionário ou amigo está indo ver o carro. Enquanto isso, o comprador acredita estar olhando o carro com algum conhecido do suposto vendedor. Ambas as partes são instruídas a não falar de preço nessa visita, o que é uma característica típica do golpe do intermediário.

Com a visita feita, o fraudador fecha o negócio com o comprador e pede o pagamento em forma de depósito ou transferência. Se a vítima aceita os termos da negociação, os golpistas então fornecem uma ou algumas contas bancárias que não pertencem ao usuário que originalmente anunciou o item na plataforma. No caso de venda de veículos, eles também orientam o comprador a ir até um cartório e preencher um recibo, tudo para dar mais veracidade ao golpe. O comprador, achando que está pagando pelo veículo, faz o repasse para o criminoso.

Quando as vítimas percebem o esquema, o recibo já foi preenchido e todo o dinheiro da negociação foi para a conta dos criminosos, que realizam o saque logo em seguida, impedindo a recuperação do dinheiro.

DICA DA PCRS:

- Desconfie de ofertas muito boas, como um carro em excelentes condições e com valor abaixo do mercado.

- Dê preferência para anúncios com perfil verificado.

- Não negocie com intermediários, dê preferência a negociar diretamente com o dono do veículo.

- Da mesma forma, se você for um vendedor, negocie apenas com o interessado no veículo, e recuse visitas de terceiros.

- Suspeite de negociações que, além de possuir terceiros, pedem sigilo acerca dos valores negociados entre as partes.

-Desconfie de histórias contadas pela outra pessoa da negociação acerca de valores que irá receber de uma rescisão no trabalho ou dívidas de amigos e familiares

- Antes de efetivar qualquer compra, procure ver o objeto anunciado pessoalmente, preferencialmente em local público, movimentado e durante o dia.

- Quando for realizar o pagamento, verifique o nome, o CPF e o número da conta do beneficiário. No caso do comprador, confirme os dados e faça transferência apenas para a conta bancária do proprietário do veículo ou seu representante legal.

GOLPE DO FALSO SITE DE INTERNET:

COMO FUNCIONA O GOLPE:

Para aplicar este golpe, os criminosos criam sites falsos de venda de mercadorias, principalmente de aparelhos eletrônicos e de eletrodomésticos. Para despertar menos suspeitas, são utilizados endereços de empresas famosas, alterando apenas o final do endereço eletrônico. A aparência do site também é idêntica ou muito similar a de sites conhecidos, tudo visando aumentar as chances de enganar a vítima. Este tipo de golpe costuma ter maior incidência em datas comemorativas e promocionais, como a Black Friday, por exemplo.

DICA DA PCRS:

- Observe com cuidado todo o endereço eletrônico.

- Mesmo que seja um perfil conhecido, sugere-se que só se efetue o pagamento após conversar diretamente com a pessoa

- Observe selo e certificados de segurança.

- Pesquise a reputação da empresa eletrônica em que pretende efetuar a compra.

- Verifique comentários de outros consumidores nas redes sociais.

- Desconfie de objetos ou serviços que estão sendo oferecidos por preço muito abaixo daquele praticado no mercado.

- Desconfie se o site só aceitar pagamento por boleto ou transferência, se tiver falhas ou erros na página e se o único contato for por WhatsAppticado no mercado.

GOLPE DO DEPÓSITO COM ENVELOPE VAZIO:

COMO FUNCIONA O GOLPE:

Este golpe tem início geralmente após a vítima fazer um anúncio para venda de um determinado bem ou objeto em um site de compras ou nas redes sociais. Após a negociação, o criminoso **realiza um depósito em um caixa eletrônico sem colocar nenhum recurso, seja dinheiro ou cheque, dentro do envelope**. Desta forma, ele obtém um comprovante de depósito, mesmo sem utilizar qualquer quantia.

Como a verificação bancária do depósito pode demorar algumas horas ou, em alguns casos, até um dia útil, o valor aparece como depositado até que o banco ateste que o pagamento não foi efetivamente realizado. Nestes casos, normalmente o criminoso já retirou o produto ou enviou um motorista por aplicativo para coletar o objeto.

DICA DA PCRS:

- Quando realizar 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.

- Os criminosos podem ser convincentes, por isso, sempre **duvide e desconfie de propostas que aparentam ser muito boas**, mais do que o comum para negócios ou produtos do mesmo tipo.

- Tenha sempre calma antes de fechar qualquer negócio. Verifique bem os temos e dados apresentados pelo interlocutor. Ter pressa pode acarretar em grandes prejuízos.

GOLPE DO FALSO SEQUESTRO:

COMO FUNCIONA O GOLPE:

Neste tipo de crime, o golpista, que normalmente já se encontra preso, liga de maneira aleatória para diversos números. A vítima atende e alguém simula uma voz de choro e medo, chama mãe ou pai, e diz que foi sequestrado. Assustada, a pessoa que atende ao telefonema costuma falar o nome de um filho, sobrinho ou de alguém próximo, mesmo sem perceber. Quando isso acontece, a própria vítima começa a passar informações que ajudam o criminoso a preencher as lacunas para completar o golpe. Com essas informações, o bandido faz a pessoa acreditar, cada vez mais, que se trata de um sequestro verdadeiro. A partir daí, o criminoso mantém a vítima na linha e pede que sejam realizadas transferências bancárias para a conta de algum laranja.

DICA DA PCRS:

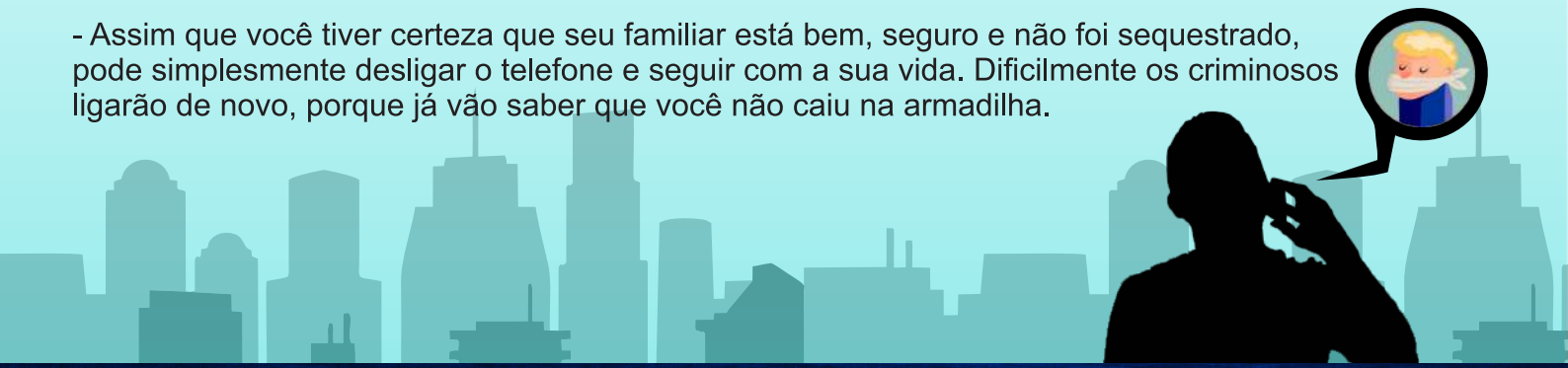
- Em primeiro lugar, é preciso superar o choque inicial e manter a cabeça fria. Pergunte a si mesmo se faz sentido alguém da sua família ter sido sequestrado naquele momento. Onde estão seus familiares? Na escola? No trabalho?

- Outra dica importante: não fale o nome da pessoa que poderia ter sido sequestrada. Dessa forma você evita passar para os criminosos informações que eles podem usar para deixar o golpe mais realista.

- Além de não mencionar nomes — pelo menos nenhum nome verdadeiro —, não passe nenhuma informação pessoal sua ou de seus familiares. Não diga, por exemplo, onde mora, o seu nome, quanto ganha, quanto tem na sua conta bancária ou onde tem conta

- Caso tenha receio de desligar acreditando ser verdadeiro o sequestro, peça para que alguém próximo, como um familiar ou vizinho, faça contato com a suposta vítima para saber se está tudo bem.

- Assim que você tiver certeza que seu familiar está bem, seguro e não foi sequestrado, pode simplesmente desligar o telefone e seguir com a sua vida. Dificilmente os criminosos ligarão de novo, porque já vão saber que você não caiu na armadilha.



GOLPE DA CLONAGEM DO WHATSAPP:

COMO FUNCIONA O GOLPE:

Este crime tem início com a obtenção do número de celular da vítima. Os golpistas têm diversos meios de conseguir essa informação, mas o mais usual é que seja retirado de anúncios em sites de compras ou anúncios públicos em redes sociais.

Na posse do número de telefone, o criminoso tenta ativar o Whatsapp da vítima no aparelho dele. Para efetivar esse procedimento, ele entra em contato com o usuário e se passa por funcionário da plataforma de anúncio ou de empresas conhecidas, utilizando como argumento a necessidade de ativar o anúncio ou confirmar dados do cadastro, por exemplo. O golpista, então, solicita um código de 6 dígitos, enviado por SMS à vítima. É esse código que vai liberar o acesso ao Whatsapp do usuário, que, por sua vez, perde o acesso ao aplicativo.

Na etapa seguinte, o criminoso, que já roubou a conta do aplicativo, inicia conversas com contatos da vítima, se passando por ela, e solicita dinheiro emprestado. Esses contatos, 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 vítimas do golpe.

DICA DA PCRS:

- Passo fundamental para evitar cair nesse tipo de golpe é habilitar a verificação em duas etapas do Whatsapp. Essa opção normalmente fica disponível no menu do aplicativo, dentro da opção “Conta” e em “Confirmação em duas Etapas”. Depois, toque em “ativar” e finalize criando uma senha de seis dígitos e informando um email pessoal.

A autenticação em dois fatores é uma medida que garante proteção extra em aplicativos. Com o recurso, mesmo que o golpista tenha acesso ao código de autenticação para ativar a conta da vítima em outro dispositivo, o serviço exigirá a senha personalizada do usuário. Além disso, também impossibilitará que o criminoso use o recurso de “esqueci minha senha” para modificar o acesso à conta da vítima.

- Não repasse código recebidos por SMS, isto é, jamais informe para qualquer pessoa o código de 6 números que chegar por torpedo SMS.

- Caso tenha informado o código e caído no golpe, é necessário enviar um e-mail à plataforma explicando o ocorrido, informando o seu número de telefone e solicitando a desativação temporária da conta.

- Caso 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. Caso seja verdade, antes de qualquer confirmação de depósito, confirme os dados do destinatário (nome, CPF, agência bancária).

GOLPE DO BILHETE PREMIADO:

COMO FUNCIONA O GOLPE:

Este golpe se inicia com a vítima, em geral uma pessoa idosa, sendo abordada na rua por uma pessoa humilde, que pede algumas informações e diz ter um bilhete de loteria premiado. Há casos, também, em que o "bilhete" é substituído por um precatório ou uma herança a receber.

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 dinheiro ou ainda que tem ações na Justiça que o impediriam de receber a premiação. Em seguida, entra em cena um segundo criminoso. Esse sujeito, mais bem-arrumado, alega ter ouvido toda a conversa e simula falar com alguém da Caixa Econômica Federal para confirmar a veracidade do prêmio.

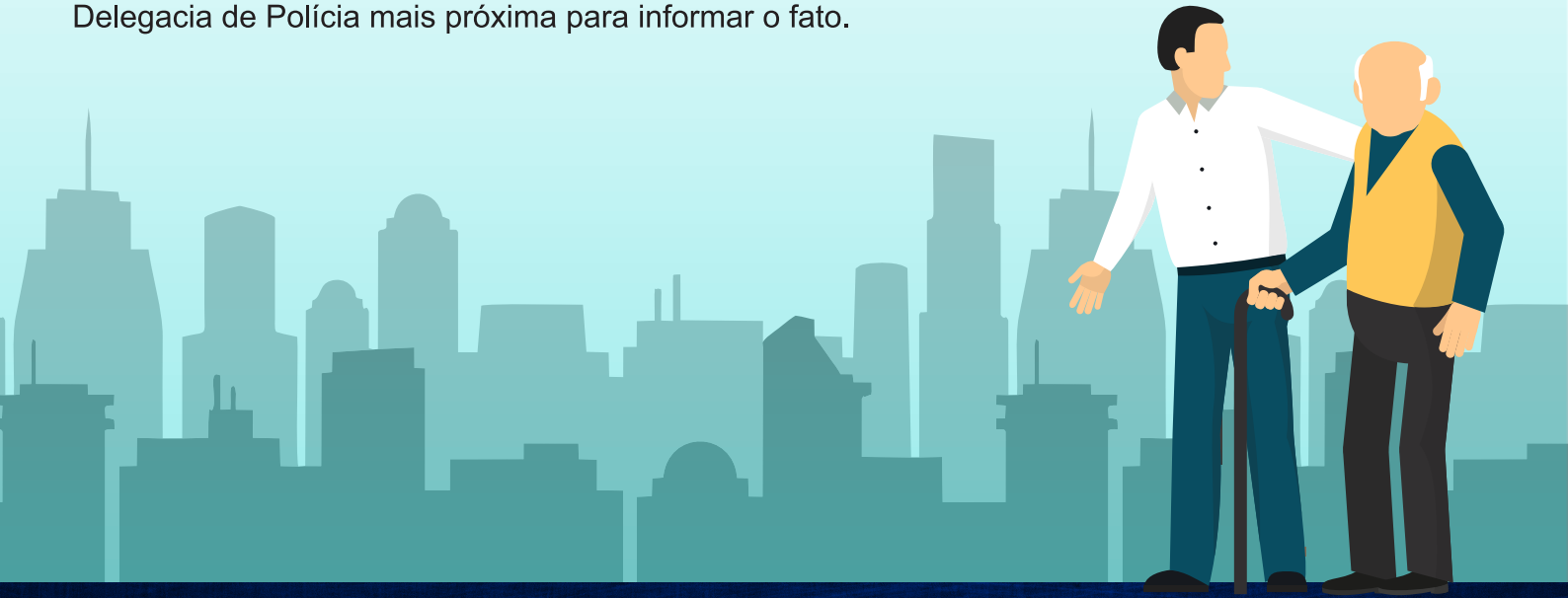
Na sequência, os golpistas convencem a vítima a transferir valores, entregar cartões e outros itens para o falso vencedor, como garantia para o recebimento do prêmio. A vítima, nesses casos, acredita que ficará com parte do valor a ser recebido. Geralmente, eles acompanham a vítima até uma agência bancária para fazer o saque ou transferência, por isso, esse crime acaba acontecendo nas proximidades de agências bancárias.

Ao final, eles então entregam o bilhete, que não possui, obviamente, nenhuma premiação.

DICA DA PCRS:

- Não existe ganho de dinheiro fácil, ainda mais em abordagens na rua por desconhecidos. Sempre desconfie de propostas desse tipo, por mais convincentes que pareçam.

- Caso alguém peça ajuda em alguma situação semelhante, diga que não pode ajudar e procure a Delegacia de Polícia mais próxima para informar o fato.



GOLPE DO CARTÃO DE CRÉDITO CLONADO:

COMO FUNCIONA O GOLPE:

O golpista faz contato com a vítima e se apresenta como funcionário de uma administradora de cartão de crédito. Ele informa que houve uma compra duvidosa no cartão da vítima e solicita que a pessoa confirme ou não a transação. Quando a vítima nega ter feito as transações e pede o cancelamento da operação, o "funcionário" informa que provavelmente houve uma clonagem e que, por isso, será necessário bloquear o cartão. O criminoso solicita, então, que seja realizada uma ligação para o 0800 da administradora para realizar o procedimento.

O ponto fundamental deste golpe, no entanto, é que o golpista que está na linha não finaliza a ligação. O cliente do cartão disca para o atendimento da empresa e o criminoso coloca uma gravação como se fosse do banco. Na sequência, acreditando que está falando com uma pessoa da administradora, a vítima fornece dados pessoais e do cartão de crédito, incluindo senha e o código verificador (os três dígitos de segurança que ficam no verso). Depois de obter estas informações, o suposto atendente da empresa informa que enviará um funcionário ou motoboy que trabalha para o banco para recolher o cartão clonado. A vítima, então, dá o cartão cortado em duas partes, mas com os dados ainda legíveis e chip intacto. Com o cartão em mãos e sabendo os dados pessoais do cliente, os golpistas fazem compras em diversas lojas físicas e virtuais.

DICA DA PCRS:

- Instituições financeiras não recolhem cartões dos clientes, mesmo que estejam vencidos ou inutilizados.

- Da mesma forma, os bancos também não solicitam informações sensíveis por telefone. Não forneça nem digite seus dados.

- Se for descartar seu cartão por qualquer motivo, corte sempre o chip ao meio. Desta forma, você garante que ele não seja utilizado por outras pessoas. O ideal é que você mesmo realize esse procedimento, para evitar que outras pessoas tenham acesso ao cartão.

- Caso você receba alguma ligação de qualquer loja, instituição financeira ou administradora de cartão de crédito informando que seu cartão foi clonado ou desejando a confirmação de alguma compra que você não tenha feito, procure a sua agência bancária ou faça contato com o seu gerente de conta.

GOLPE DA TROCA DE CARTÃO:

COMO FUNCIONA O GOLPE:

A vítima, após ser observada inserindo os dados do cartão no caixa eletrônico, é abordada na saída da agência bancária por alguém que se apresenta como funcionário do banco. Essa pessoa normalmente está bem-vestida e apresenta um crachá de identificação. Ela informa que houve algum problema na transação efetuada ou na máquina e solicita que a vítima retome ao caixa eletrônico para verificarem. Neste momento, o golpista finge auxiliar o cliente e rapidamente efetua a troca do cartão. Em alguns casos, o criminoso 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:

O golpe consiste na emissão de um boleto bancário falso a partir da manipulação do código de barras do documento ou a partir de uma falsa página de loja virtual. Em alguns casos, os criminosos também podem fazer contato com a vítima pelo WhatsApp para realizar uma falsa venda. O documento adulterado possui cabeçalho e imagens da loja ou empresa com a qual a vítima estava negociando. O valor transferido ou pago por meio do boleto falso 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 ou empresa.

- Caso queira emitir uma 2º 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 com propostas tentadoras. Normalmente são oferecidos crédito fácil e rápido, juros mais baixos do que aqueles operados por instituições financeiras, possibilidade de pagamento em diversas parcelas, sem consulta ao SPC/Serasa e liberação de crédito mesmo a vítima estando negativada.

A partir do momento que a pessoa manifesta interesse na proposta, os criminosos passam a cobrar uma taxa para que haja a liberação do crédito. Entre as alegações utilizadas por eles para justificar o pagamento, estão supostas taxas de abertura de crédito, taxas exigidas pelo Banco Central, seguros de crédito, entre outras cobranças falsas.

DICA DA PCRS:

- Instituições bancárias e financeiras não solicitam depósito prévio. Se houver alguma solicitação nesse sentido, é indício de que se trata de um golpe.

- Não confie em ganhos fáceis e promessas extremamente vantajosas, especialmente se você não procurou uma instituição financeira.

- Antes de realizar qualquer contrato, procure sempre pesquisar o nome da instituição na internet e em sites que registram queixas dos consumidores, como o Reclame Aqui ou o Procon, por exemplo.

- Mesmo diante da facilidade de resolver tudo virtualmente, opte, sempre que possível, por fazer 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 GOgolpe:

Para aplicar esse golpe, os criminosos fazem uso das redes sociais. As vítimas podem ser homens ou mulheres, mas, mais usualmente, costumam ser homens, maiores de idade e muitas vezes casados. O golpista cria um perfil falso, na maioria das vezes com a foto de uma jovem bonita e atraente. Na sequência, ele solicita amizade ou faz contato por mensagem com a vítima, com quem troca fotos íntimas. De posse dessas imagens, um segundo criminoso passa a fazer contato com a vítima, se passando por pai ou padastro da jovem. Ele então alega que a moça é menor de idade e que, portanto, a vítima estaria praticando o crime de pedofilia pela internet. A partir daí, esse criminoso passa a exigir o pagamento de uma quantia. O valor seria para evitar que o caso seja levado à Polícia ou mesmo para que a esposa/marido da vítima não fique sabendo da situação. Há casos, ainda, em que os golpistas se passam por policiais civis, utilizando nomes de servidores reais e alegando que as fotos já fazem parte de um Inquérito Policial. Eles, então, solicitam um depósito para que a investigação seja "arquivada".

DICA DA PCRS:

- Não troque nem compartilhe fotos íntimas pela internet. Lembre-se: uma foto ou um vídeo compartilhado pode circular entre milhares de pessoas.

- Desconfie de solicitações de amizades de pessoas que você não conhece.

- Armazenamento de material pornográfico infanto juvenil é crime, portanto, se a pessoa com quem você está fazendo uma nova amizade aparenta ser menor de idade, todo o cuidado é necessário.

- Delegados e agentes da Polícia Civil não fazem contato por WhatsApp para tratar sobre investigações, muito menos para solicitar vantagens financeiras. Caso receba alguma abordagem nesse sentido, bloqueie o contato e registre boletim de ocorrência.

- Caso tenha caído no golpe e já tenha realizado alguma transferência, bloqueie o contato do criminoso, registre boletim de ocorrência na Delegacia de Polícia mais próxima e entre em contato com sua instituição financeira para informar sobre o golpe.

GOLPE DO NUDE:

COMO FUNCIONA O Ggolpe:

O criminoso cria perfis falsos em redes sociais, na maioria das vezes com a foto de uma jovem bonita e atraente.

Na sequência, ele solicita amizade da vítima, com quem passa a trocar fotos íntimas.

De posse dessas imagens, é iniciada a extorsão. O golpista contata a vítima, normalmente por WhatsApp, se passando por pai ou padrasto da suposta jovem e passa a exigir dinheiro, alegando que a mulher é menor de idade. O valor seria para evitar que o caso seja levado à Polícia ou a público. Há casos em que os criminosos se passam por policiais civis, usando nomes de servidores reais.

DICA DA PCRS:

- Não troque ou compartilhe fotos íntimas pela internet, especialmente com pessoas que só conhece virtualmente;

- Desconfie de solicitações de amizade de pessoas que você não conhece;

- Pedofilia é crime, portanto, se a pessoa com quem você está fazendo uma nova amizade aparenta ser menor de idade, todo o cuidado é necessário;

- Caso tenha caído no golpe, bloqueie o contato do criminoso;

- Procure a Delegacia de Polícia mais próxima ou acesse o site da Delegacia Online e registre boletim de ocorrência;

- Denuncie o perfil da rede social para a plataforma responsável;

- Se tiver feito transferências bancárias, entre em contato com sua instituição financeira para informar sobre o crime;

GOLPE DO PARENTE QUE QUEBROU O CARRO:

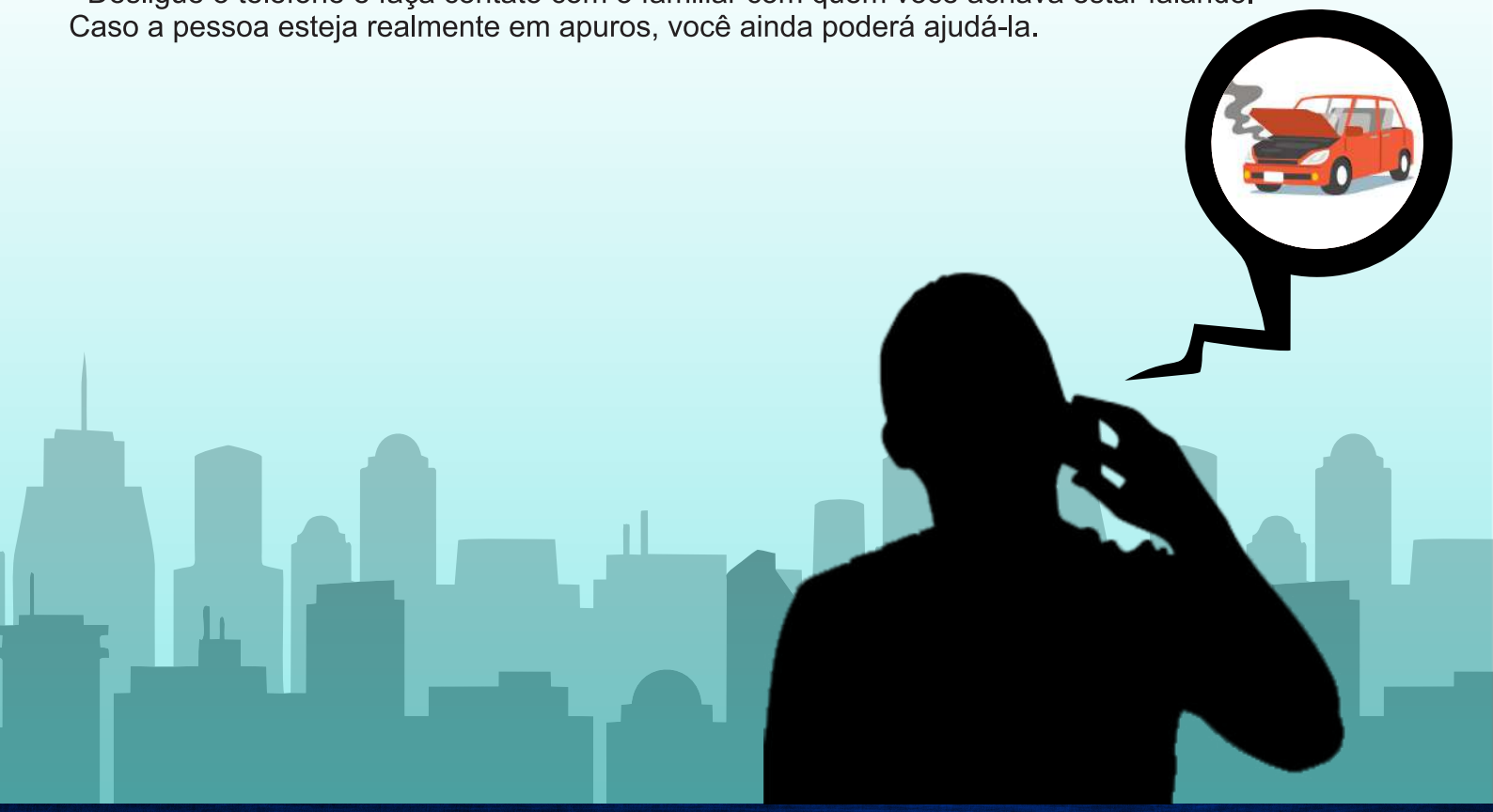
COMO FUNCIONA O Ggolpe:

O golpista liga aleatoriamente para as vítimas e, ao ser atendido, usa frases genéricas como “oi tio/tia, sabe quem está falando?”. Caso a vítima diga um nome, achando ser algum sobrinho ou parente distante, o criminoso utiliza esta informação para prosseguir com o golpe. Ele então diz que seu carro quebrou e que precisa de ajuda, solicitando uma transferência para pagamento de mecânico, ferragem ou borracharia, por exemplo. Há casos em que a vítima diz não se recordar do suposto sobrinho. Nestes casos, os golpistas podem usar artifícios para constrangê-la por não se lembrar do “familiar”, estimulando-a a continuar a conversa.

DICA DA PCRS:

- Não faça transferências ou dê dinheiro para terceiros.

- Desligue o telefone e faça contato com o familiar com quem você achava estar falando. Caso a pessoa esteja realmente em apuros, você ainda poderá ajudá-la.



GOLPE DO BOOK FOTOGRÁFICO:

COMO FUNCIONA O GOgolpe:

Geralmente, as vítimas deste tipo de golpe são pessoas idosas. Elas são abordadas pelos golpistas com a promessa de brindes, maquiagens e fotos gratuitas. Após serem persuadidas, as vítimas aceitam fazer as fotos em pequenos estúdios. Ao final, depois de uma produção de maquiagem, trocas de roupas e diversas fotos, elas são constrangidas a pagar valores bem altos pelas fotos.

DICA DA PCRS:

- Não aceite propostas recebidas em abordagens na rua, por mais simpático e persuasivo que seja a pessoa que lhe abordou

- Se você está interessada em fazer um book fotográfico, procure uma empresa séria e pesquise sobre a reputação na internet.

GOLPE DO PIX:

COMO FUNCIONA O GOLPE:

O Pix foi lançado em novembro de 2020 como forma de simplificar e facilitar transações financeiras e, desde então, também entrou na mira de criminosos. Em um dos crimes mais recentes que se utilizam dessa tecnologia, o golpista contata a vítima se passando por atendente de banco. Em seguida, ele informa o “cliente” que sua conta foi bloqueada por tentativa de invasão e promete uma solução rápida para o problema. Um dos principais aspectos desse golpe é que o criminoso cita valores reais movimentados pelo cliente, o que passa veracidade durante o contato. Um dos montantes informados por ele, no entanto, não é reconhecido pela vítima. Por isso, ele solicita que seja realizada uma transferência via Pix no mesmo valor informado. Para justificar esse pedido, o criminoso alega que uma transferência “duplicada” será cancelada pelo banco. A chave Pix é enviada para a vítima por mensagem.

DICA DA PCRS:

- Caso receba esse tipo de abordagem, finalize a ligação e procure algum contato oficial do banco para que possa tirar suas dúvidas. Se possível, faça a ligação de outro aparelho telefônico.

- Não informe dados nem digite senhas sigilosas em ligações telefônicas, mesmo que citem informações, a primeira vista, corretas. Bancos, eventualmente, podem contatar clientes para verificar transações, mas não solicitam dados sigilosos nem transferências.

- Não clique em links recebidos por Whatsapp ou SMS e tampouco informe dados recebidos por mensagem para terceiros.

GOLPE DO PIX REVERSO:

COMO FUNCIONA O GOgolpe:

Neste golpe, o criminoso forja um comprovante de transferência via Pix de determinado banco e o envia por e-mail ou WhatsApp da vítima. Ao receber o falso print, a pessoa estranha a mensagem e pergunta do que se trata. O golpista, então, diz que errou ao fazer a transferência e pede à vítima para reembolsar o valor para a conta dele. Por meio desse "Pix reverso", além de não ter depositado dinheiro algum na conta da vítima, o criminoso ainda tenta fazer com que a vítima lhe pague uma quantia.

DICA DA PCRS:

- Para não ser vítima do golpe do Pix reverso, basta abrir o aplicativo do banco e verificar se houve de fato algum pagamento. Se o valor não constar dos recebimentos, trata-se de fraude.

DICAS FINAIS DA POLÍCIA CIVIL RS:

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 e serviços com preços abaixo dos praticados em mercado;

3. Não converse com estranhos na rua, tampouco aceite propostas que pareçam ser muito boas e que lhe trariam alguma espécie de “vantagem”;

4. A aparência pode enganar. Estelionatários falam bem, estão normalmente bem-vestidos e facilmente persuadem as vítimas.

5. Não troque fotos nem vídeos íntimos pela internet ou rede social. Se a pessoa com quem conversa aparenta ser menor de idade, reforce ainda mais os cuidados. Lembre-se: armazenamento de material pornográfico infanto-juvenil 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, pelo WhatsApp da Polícia Civil, no número (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. Você também pode registrar a ocorrência pela Delegacia Online:
www.delegaciaonline.rs.gov.br