OAB MATO GROSSO 90 ANOS | Comissão de Direito Bancário

CARTILHA FRAUDES BANCÁRIAS

Comissão Estadual de Direito Bancário da OAB/MT

Autores:
- André Luiz Campos das Neves Ribeiro
- Angélica Anai Angulo
- Bruno Felipe Monteiro Coelho (coord.)
- Diogo de Oliveira da Cruz
- João Carlos Disarsz Alves
- Santiany Almeida de Siqueira Curvo

SUMÁRIO

1. O que são fraudes bancárias 3

2. Espécies de fraudes 4

2.1 Golpe do PIX 4

2.2 Golpe do Motoboy 5

2.3 Golpe da Mão Fantasma 6

2.4 Golpe do Boleto Falso 6

2.5 Phising e SMishing Bancário 7

2.6 Golpe da falsa central de atendimento 7

2.7 Golpe do falso leilão 7

2.8 Golpe no WhatsApp 7

2.9 Golpe da troca de cartão 8

2.10 Site, Link ou Perfil/Pág. de Rede Social Falsa das Instituições Bancárias 8

2.11 Golpe do Falso Protesto 8

2.12 Golpe do depósito prévio para liberação de empréstimo 8

3. Soluções e combate às fraudes 9

3.1 principais formas de identificar uma fraude e como se proteger 9

3.2 cuidados antes de passar qualquer informação pessoal 11

3.3 canais de atendimento e auxílio ao consumidor 12

3.4 principais medidas em caso de suspeita de fraude 12

4. O que fazer se tiver sofrido algum destes golpes 13

O QUE SÃO FRAUDES BANCÁRIAS

A fraude em sua definição consiste em qualquer ato ardiloso, enganoso, de má-fé, com o intuito de lesar ou ludibriar alguém, ou de não cumprir determinado dever.

Como conduta, a fraude possui reprovação da sua efetivação junto ao Código Penal, mais especificamente no seu art. 171, que define como crime a prática de "obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento". As penas nesse caso podem chegar até cinco anos de reclusão.

No universo das relações civis, os contratos que de algum modo sejam submetidos a essa prática fraudulenta, podem ser anulados, se demonstrado que alguma das partes foi levada a erro, o que geralmente se caracteriza pela alteração do objeto do negócio firmado.

As relações envolvendo o Direito Bancário, quando evidente a existência de consumidor final, são, por força da súmula 297 do STJ abarcadas pelo Código de Defesa do Consumidor, que define a teoria da responsabilidade objetiva, ou seja, com a responsabilização independentemente de culpa, como marco para análise de circunstâncias e responsabilização de eventuais atos fraudulentos sofridos pelos consumidores. Nesse aspecto, inúmeros são o julgados que protegem o consumidor de relações rotineiras, de transações bancária fraudulentas, mesmo sem a participação da instituição bancária.

No Direito Bancário, por envolver relação entre o proprietário e detentor do dinheiro depositados nas contas correntes ou de direito para essa obtenção, facilmente nos deparamos com condutas de terceiros que buscam alterar, com o uso de tecnologia, a finalidade de algumas transações bancárias, dentre elas, o pagamento, transferências, contratações de empréstimos ou serviços, bem como obtenção indevida de dados sigilosos.

É nessa condição que entendemos as fraudes bancárias como sendo aquela que de qualquer sorte buscam alterar a finalidade das atividades envolvendo as relações entre correntistas (consumidores) e instituição bancária.

ESPÉCIES DE FRAUDE

Há diversas modalidades de fraude bancária, e compete trazer o conhecimento de forma clara e intuitiva a fim de que possamos repassar um pouco mais do conhecimento acerca das espécies e as características das fraudes utilizadas pelos estelionatários a fim de que possamos evitar as referidas fraudes.

Nesse trabalho produzido pela Comissão de Direito Bancário da OAB/MT, selecionamos as 12 principais fraudes bancárias ocorridas atualmente, bem como as suas características e meios de evitá-las.

GOLPE DO PIX

Com mais de 550 milhões de chaves cadastradas até Dezembro de 2022, o Pix foi aceito de forma muito fácil pela população brasileira, tendo esta consolidado a utilização do novo método de pagamento. O PIX foi lançado em novembro de 2020, e de acordo com as estatísticas do Banco Central 141,6 milhões de pessoas utilizam o serviço, possuindo o referido cadastro.

A alta adesão é evidenciada pela praticidade, facilidade e instantaneidade oferecidas pelos pagamentos via PIX, fato este que atrai também os fraudadores. A partir destas facilidades os criminosos possuem diversos métodos para obter as vantagens ilícitas, partindo de roubo digital, com furto de senhas por meio do phishing (ameaça virtual), ou mensagens em WhatsApp que servem como isca para invadir o celular ou computador. Até a denominada "engenharia social", onde a intenção é enganar a vítima por meio de um contato pessoal, para então conseguir informações que permitam falsear uma identidade para as instituições financeiras. Assim destacamos os cinco principais golpes do Pix e como se proteger.

CAPTURADOR DE SESSÕES

Essa modalidade de fraude consiste no envio de um PDF ou um e-mail para a vítima com um arquivo que, se aberto, infecta o dispositivo ou computador com um vírus que notifica o criminoso quando um aplicativo ou o site do banco é aberto, permitindo assim a captura das credenciais de acesso da conta bancária.

SMS FRAUDULENTO

O golpe do SMS Emergencial é uma fraude não muito usual pela sua baixa efetividade, mas ainda assim é utilizado pelos golpistas. Os criminosos disparam milhares de SMS pedindo socorro e solicitando uma transferência via PIX, para auxiliar alguma demanda emergencial ou solucionar um problema financeiro urgente.

CLONAGEM DE WHATSAPP

A clonagem de WhatsApp é um ataque comum mesmo antes da existência do PIX. O golpe funciona da seguinte maneira: o criminoso entra em contato com a vítima fingindo ser representante de uma empresa em que a pessoa tem algum tipo de cadastro e solicita um código de segurança que é enviado por SMS supostamente para manutenção, atualização ou confirmação de cadastro. Esse código permite a clonagem do WhatsApp. A partir disso, os golpistas começam a enviar mensagens para os contatos da vítima pedindo ajuda financeira por transferência via Pix.

PERFIL FALSO DO WHATSAPP

Outra meio pelo qual os fraudadores aplicam o golpe se relaciona a clonagem do WhatsApp, nessa fraude o criminoso consegue criar uma conta nova por intermédio de informações e fotos encontradas em redes sociais da vítima. Depois de conseguir os contatos, o golpista utiliza um número desconhecido alegando que algo emergencial aconteceu, como um assalto, ou utilização do novo número apenas para utilização pessoal e o antigo para o trabalho, para justificar o número novo e assim poder pedir dinheiro aos contatos via transferência Pix.

GOLPE COM QR CODE

Nessa modalidade os criminosos enviam faturas falsificadas para as vítimas com QR Code para que sejam pagas via Pix. Geralmente são faturas de contas com serviços utilizados pelo usuário. Os golpistas imitam o visual das faturas e dos sites das empresas e oferecem descontos para que o pagamento seja realizado por meio do QR Code, a fim de incentivar que o pagamento seja feito dessa forma. Além disso, golpes também estão sendo realizados através de e-mails enviados com ofertas e planos mais em conta em serviços com pagamento via QR Code.

GOLPE DO MOTOBOY

Esse golpe é uma modalidade antiga na qual uma pessoa recebe uma ligação de um fraudador se passando pelo seu banco, dizendo que seu cartão foi clonado e que irão encaminhar um motoboy para recolher o cartão para efetivação do bloqueio. A sofisticação é tamanha que criminosos usam até mesmo softwares para simular músicas de espera de bancos e som ambiente de call center, além de conseguirem reter a linha telefônica das vítimas. Assim com a entrega do cartão ao motoboy, juntamente com os dados pessoais e senha solicitadas durante a ligação os criminosos conseguem utilizar o cartão para realizar saques, empréstimos, compras e pagamentos de boletos.

GOLPE DA MÃO FANTASMA

O golpe da mão fantasma é um golpe mais recente e possui um trato de engenharia social mais avançado, além de ser necessária a participação da própria vítima para a concretização do golpe. Incialmente a vítima recebe uma ligação na qual a gravação aparenta ser àquelas provenientes de centrais telefônicas de bancos e instituições financeiras. Ao ser transferido para um atendente, que neste caso é o próprio criminoso, o consumidor é informado que há movimentações estranhas, como uma compra suspeita e até mesmo uma possível invasão na conta. A intenção é deixar a pessoa preocupada e insegura com a informação, facilitando a aplicação do golpe.

A partir deste momento, os criminosos, se passando por funcionários dos bancos, induzem a vítima a acessar algum link para a instalação de um aplicativo que irá solucionar o problema. Ao instalar, no entanto, o criminoso passa a ter acesso a todos os dados que estão no smartphone ou no computador, a depender do local em que foi realizada a operação, inclusive os bancários. Com acesso ao aparelho, os fraudadores realizam buscas minuciosas, pesquisam por senhas armazenadas pelos próprios usuários em aplicativos e sites e, dessa forma, realizam transações fraudulentas, como transferências, pagamento de contas e boletos e solicitação de empréstimos.

GOLPE DO BOLETO FALSO

Os boletos fazem parte do dia a dia do brasileiro. Segundo o Banco Central, foram mais de 2 milhões de boletos emitidos somente nos três primeiros meses de 2022, assim é evidente que pelo costume e pela rotina os brasileiros efetivam o pagamento de inúmeros boletos diariamente e por muitas vezes não se atentam aos detalhes, abrindo caminho aos fraudadores.

Mais comumente o golpe do boleto falso utiliza dados pessoais disponíveis na internet para enviar uma cobrança fingindo ser uma empresa que você utiliza, costumeiramente as pessoas recebem um e-mail com a informação de que se encontram em débito com alguma fatura de alguma empresa de telefonia, ou banco, ou cartão de crédito e que com o referido boleto podem quitar a referida obrigação, muitas vezes com desconto, incitando a vítima a efetivar o pagamento como se estivesse quitando o seu débito.

Há também a aplicação do golpe do boleto falso para compras via internet. Geralmente os criminosos se utilizam de lojas virtuais falsas, assemelhadas com as verdadeiras, com estruturas, cores e até logomarcas semelhantes, ofertando produtos com descontos para pagamento por boleto, assim induzem a vítima a efetivarem o pagamento deste boleto para um terceiro.

Por isso, antes de se efetivar o pagamento do boleto é importante confirmar se os dados do vendedor e do beneficiário estão corretos, se o valor cobrado está alinhado com o valor que deve ser pago, se o e-mail, WhatsApp ou site que pegou o boleto é uma fonte segura e verifique também se há erros de digitação, com essas dicas será possível se precaver contra possíveis boletos fraudados

PHISING SMISHING BANCÁRIO

Phising e SMihing são uma modalidade de golpe ocorrida por meio de envio de e-mails (phising), ou mensagens de texto – SMS (smishing), fraudulentos que buscam induzir o destinatário a abrir um anexo com malware ou clicar em um link malicioso. A partir de clicado no referido link o malware é instalado tanto no seu celular quanto em seu computador, a fim de obter os dados da vítima, por meio da digitação destes dados em um programa ou em link de site falso, podendo os criminosos se utilizarem dos referidos dados para realizar fraudes em nome das vítimas.

GOLPE DA FALSA CENTRAL DE ATENDIMENTO

Nesse caso o fraudador entra em contato com a vítima se passando por um falso funcionário do banco ou empresa com a qual ela tem um relacionamento ativo. Informa que sua conta foi invadida, clonada ou outro problema e, a partir daí, solicita os dados pessoais e financeiros da vítima. E até mesmo pede para que ela ligue na central do banco, no número que aparece atrás do seu cartão, mas o fraudador continua na linha para simular o atendimento da central e pedir os dados da sua conta, dos seus cartões e, principalmente, a sua senha quando você a digitar, obtendo assim todas as informações necessárias para cometer fraudes junto a conta da vítima.

GOLPE DO FALSO LEILÃO

Esse tipo de golpe se trata da criação, pelos fraudadores de um site de leilão, de carros, motos, ônibus, caminhões e demais bens móveis, com a intenção de leiloar, expondo que os veículos foram recuperados por instituições financeiras, e aproveitando do interesse do consumidor, os criminosos criam um site falso com propostas tentadoras para aplicar o golpe nas vítimas. Visando passar a imagem de legalidade, os estelionatários, fazem o atendimento do consumidor, respondem dúvidas, fazem o cadastro junto ao site, porém, após o arremate do bem em leilão, e o pagamento, o susposto Leiloeiro passa endereço onde buscar o bem, porém o endereço é inexistente, e com isso não mais atendem o consumidor.

GOLPE NO WHATSAPP

O WhatsApp é clonado quando um cibercriminoso toma posse da conta da vítima sem ela ter conhecimento. Os golpistas ganham acesso à conta real do usuário no mensageiro em outro celular, e conseguem receber e enviar mensagens aos contatos pelo WhatsApp da vítima, se passando pela pessoa, e pedindo a seus familiares e amigos dinheiro como se fosse para pagar um conta, ou que o carro esta quebrado, ou até mesmo por questão de saúde, as necessidades são várias, todavia o intuito é o mesmo, ludibriar a pessoa a transferir o dinheiro para conta dos golpistas.

GOLPE DA TROCA DE CARTÃO

O golpe se inicia quando o cliente recebe uma ligação do golpista que se passa por funcionário do banco, dizendo que o cartão foi fraudado. O falso funcionário solicita a senha e pede que o cartão seja cortado, mas que o chip não seja danificado. Em seguida, diz que o cartão será retirado na casa do cliente, assim, o susposto motoboy se passando ser funcionário do banco, vai até a residencia da vítima e pega o cartão, com isso, os golpistas tem acesso ao numero do cartão, chip e senhas de segurança, utilizando o cartão, fazendo compras, e deixando o grande dano financeiro a vítima.

SITE, LINK OU PERFIL/PÁGINA DE REDE SOCIAL FALSA DAS INSTITUIÇÕES BANCÁRIAS

O golpe é direcionado a pessoas que possuem relação jurídica com o banco, onde a vítima ao tentar a acessar sua conta pelo site, os criminosos tentam obter as chaves de homebanking, que significa banco eletrônico ou banco on-line, e com subtração das senhas de acesso, os criminosos além de esvaziar a conta da vítima com transferência para as contas dos golpistas, também solicitam empréstimos pré-aprovados. Com o golpe, a vítima fica sem dinheiro, e com parcelas do empréstimo a pagar.

GOLPE DO FALSO PROTESTO

Os criminosos obtém a informação de dívida de um consumidor, dívidas essas muitas vezes já prescritas, e encaminham mensagens, e-mails e até telefonemas informando que aquele consumidor está com o nome protestado por esta dívida, para passar a imagem de legalidade, encaminham o título do protesto, com o brasão das entidades públicas e do suposto cartório, oferecendo vantagens aos devedores na quitação dos débitos existentes, assim, quando o consumidor tenta regularizar a situação, os falsários encaminham um boleto para pagamento, onde os valores cairão na conta dos falsários. Nesse caso, se o pagamento for feito, o envio do título de quitação não se concretiza. O prejuízo nesses casos é em dobro, já que depois a vítima precisa quitar a dívida com a pessoa ou a empresa que realmente está devendo.

GOLPE DO DEPÓSITO PRÉVIO PARA LIBERAÇÃO DE EMPRÉSTIMO

Os falsários encaminham mensagens, e-mail e até telefones oferecendo empréstimos com juros relativamente acessíveis, e sem a necessidade de estar com nome limpo, se aproveitando da necessidade da vítima em ter o dinheiro de forma rápida, muitas vezes para ser utilizado em questões de emergência, é solicitado pelos estelionatários, um depósito prévio a título de pagamento de cadastro ou seguro, impondo esse depósito como condição de liberação do empréstimo, quando é depositado o valor, o empréstimo não cai, e os atendentes/falsários não mais atendem a pessoa, que fica com o dano financeiro.

SOLUÇÕES E COMBATE ÀS FRAUDES

PRINCIPAIS FORMAS DE IDENTIFICAR UMA FRAUDE E COMO SE PROTEGER

Em geral, identificar uma fraude pode ser bem difícil. Atualmente os golpes assumem diversas formas. E, por isso, dificultam cada vez mais a possibilidade de o consumidor identificar se aquele é ou não um contato genuíno da empresa, entretanto, ainda assim é possível que, com bastante atenção, o consumidor identifique os principais sinais de fraude, seguindo as seguintes dicas:

SOLUÇÕES E COMBATE ÀS FRAUDES

A. DENTRO DO ESTABELECIMENTO BANCÁRIO OU LOTÉRICAS NÃO ACEITE AJUDA DE ESTRANHOS

Não aceitar ajuda de estranhos em bancos ou casas lotéricas. O aconselhável é sempre se dirigir a algum funcionário do estabelecimento financeiro.

SOLUÇÕES E COMBATE ÀS FRAUDES

B. DESCONFIE DE SOLICITAÇÕES DE SENHA POR TELE-FONE, CELULAR OU E-MAIL

As instituições financeiras não enviam e-mail e nem ligam para os clientes solicitando a senha do cartão de crédito ou o seu código de segurança, é necessário consignar que, essas informações são pessoais e intransferíveis e não devem ser divulgadas para terceiros. Por isso, desconfie se alguém solicitar tais informações, informando que são funcionários de bancos e outras instituições financeiras que façam essa solicitação. Lembre-se, também, de não fornecer dados pessoais (como nome do pai ou da mãe). Na dúvida compareça à agência bancária para sanar as dúvidas e evitar ser vítima de golpe.

SOLUÇÕES E COMBATE ÀS FRAUDES

C. NÃO ENTREGUE SEUS CARTÕES, MESMO QUE INUTILIZADOS

Os bancos não solicitam a devolução de cartões, mesmo em caso de bloqueio ou cancelamento, e não fazem esse tipo de retirada na residência dos clientes. Por isso, se você receber a visita de alguém que diz ser do seu banco, informe que já se desfez do cartão. Caso a tentativa de fraude aconteça por telefone, desligue imediatamente e entre em contato diretamente com a central de relacionamento da instituição financeira com outro telefone, essa dica é importante pois seu telefone pode estar com algum programa que irá direcionar a ligação para os golpistas.

SOLUÇÕES E COMBATE ÀS FRAUDES

D. MANTENHA O SEU CADASTRO ATUALIZADO

Tal dica é importante, uma vez que quando as instituições financeiras ou administradoras de cartões de crédito notam uma compra ou movimentação suspeita, elas entram em contato diretamente com o cliente para confirmar se foi ele mesmo quem fez as transações. Para que esse contato seja bem-sucedido e ajude no controle das fraudes, é importante que você mantenha seus dados sempre atualizados.

SOLUÇÕES E COMBATE ÀS FRAUDES

E. MEDIDAS DE PROTEÇÃO PARA EVITAR OS GOLPES

Não aceitar ajuda de estranhos em bancos ou casas lotéricas. O aconselhável é sempre se dirigir a algum funcionário do estabelecimento financeiro.

- Não clique em links suspeitos, seja por e-mail ou via SMS. Desconfie sempre da ortografia, confira o remetente corretamente;

- Para ajudar a evitar que o WhatsApp seja clonado, habilite no aplicativo a opção “Verificação em duas etapas”: Configurações > Ajustes > Conta > Verificação em duas etapas;

- No caso de receber mensagens de números novos mesmo que contenha a foto de um amigo ou familiar, desconfie caso as mensagens sejam com pedidos financeiros;

- Confira se o site em que está navegando é seguro clicando no cadeado que fica na barra de endereço do navegador;

- Baixe um antivírus para o seu dispositivo;

- Desconfie de ligações recebidas de centrais de atendimento que visem obter os seus dados;

- Nunca forneça seus dados, senhas, número de cartões, ou quaisquer outras informações por telefone;

- Nunca devolva ou entregue o seu cartão para ninguém, pois o banco nunca solicita a devolução do seu cartão;

- Desconfie de qualquer pessoa estranha que venha oferecer ajuda;

- Sempre pesquise se o site em que está realizando a operação é verdadeiro, pesquisando reclamações sobre ele, bem como a existência do cadeado de segurança no navegador;

- Sempre confira os dados do pagamento do boleto, como número do boleto, beneficiário, valor, ou seja, todos os dados, antes de completar o pagamento junto à instituição financeira;

- Antes de realizar qualquer transferência, confirme com a pessoa por meio de ligação telefônica se é ela mesmo que está solicitando a referida transferência;

- Não anote as suas senhas em locais fáceis de localização e nem em bloco de notas dentro de computadores ou celulares. De preferência utilize senhas fortes e troque-as regularmente;

- Nunca repasse códigos recebidos por SMS para terceiros.

Estes cuidados podem ser tomados e são dicas importantes, para que todos possam evitar a ocorrência dos referidos golpes. Importante destacar que os golpes ficam diariamente mais sofisticados, por isso é necessário o máximo de atenção possível nas transações bancárias.

SOLUÇÕES E COMBATE ÀS FRAUDES

CUIDADOS ANTES DE PASSAR QUALQUER INFORMAÇÃO PESSOAL

Com o crescimento do uso das tecnológicas, atualmente é possível fazer praticamente qualquer coisa online, incluindo acessar sua conta bancária, estudar e buscar entretenimento. Porém, para isso, é necessário que você realize uma série de cadastros de informações pessoais, como seu nome, endereço, documentos, dados bancários, entre outros. E saiba que esses dados pessoais são muito visados por criminosos que realizam fraudes.

SOLUÇÕES E COMBATE ÀS FRAUDES

A. PERGUNTAR O MOTIVO PELO QUAL A EMPRESA PEDIU SEU CPF:

Sabe quele pedido me informe seu CPF para fazer um cadastro, por acaso você foi informado qual seria a finalidade e qual a hipótese de tratamento de acordo com a determinação da LGPD? Entenda que toda empresa deve informar a finalidade, a hipótese de tratamento, se há compartilhamento e quais as medidas de segurança para que esse dado não seja vazado ou tenha acesso de pessoa não autorizada. Então, pergunte tudo isso. Se o atendente não souber responder, **NÃO ENTREGUE SEUS DADOS**.

SOLUÇÕES E COMBATE ÀS FRAUDES

B. NÃO PREENCHA CADASTROS DE EMPRESAS QUE VOCÊ NÃO CONHECE:

Inicialmente, por mais que a oferta seja tentadora, é necessário conferir se o site é confiável, vez que, na internet é muito fácil algum criminoso abrir sites na internet bem elaborados apenas com o intuito de coleta de dados para aplicar golpes posteriormente. Esses dados entregues para pessoas mal-intencionadas podem inclusive trazer sérios problemas como a abertura de empresas em seu nome, realização de empréstimos e financiamentos se passando por você. Assim, não informe seus dados em sites que você não conhece a procedência.

SOLUÇÕES E COMBATE ÀS FRAUDES

CANAIS DE ATENDIMENTO E AUXÍLIO AO CONSUMIDOR

Em Mato Grosso, existem canais para que o consumidor vítima de alguma fraude pode utilizar para se resguardar e ter sua denúncia entregue para as Autoridades Competentes, vejamos:

- **Consumidor.Gov.Br** que é uma ferramenta do Ministério da Justiça para auxiliar o Consumidor a resolver os seus problemas com os grandes fornecedores, basta acessar o site: https://consumidor.gov.br

- **PROCON - MT** – Endereço: Rua Baltazar Navarros, n. 567 (antigo Sine), Bairro Bandeirantes, Cuiabá - MT | CEP 78010-020 Tel.: (65) 3613-2100 Atendimento por agendamento: WhatsApp (65) 99228-3098.

- **Delegacia Virtual de Mato Grosso** no site: https://portal.sesp.mt.gov.br/delegacia-web/pages/home.seam

- **Delegacia Especializada de Defesa do Consumidor – DECON** - Endereço: Av. Dante Martins de Oliveira, s/nº, bairro Planalto – Cuiabá / MT Telefones: (65) 3901-4809 E-mail: decon@pjc.mt.gov.br

- **Delegacia Especializada de Estelionato e Outras Fraudes de Cuiabá.** Av. Dante Martins de Oliveira, s/n, bairro Planalto - Cuiabá / MT Telefones: (65) 3901-4220 (protocolo) e (65) 3901-4232 (cartório central) E-mail: dpestelionato@pjc.mt.gov.br

SOLUÇÕES E COMBATE ÀS FRAUDES

PRINCIPAIS MEDIDAS EM CASO DE SUSPEITA DE FRAUDE

Se tiver sofrido um golpe ou tenha ocorrido alguma transação suspeita em sua conta bancária, quanto mais rápido a vítima agir maior as chances de recuperar o dano. Conheça o passo-a-passo:

a. Registre imediatamente a reclamação no site em que ocorreu o problema;

b. Recupere os registros e protocolos para entrar em contato com a empresa;

c. Registre a reclamação no site do Ministério da Justiça (http://consumidor.gov.br/) ou procure o PROCON de sua cidade;

d. Faça um boletim de ocorrência;

e. Caso haja fraudes em sua conta bancária ou cartão de crédito, comunique imediatamente seu banco para cancelar as transações com o boletim de ocorrência em mãos;

f. Mantenha seu antivírus sempre atualizado também para bloquear programas maliciosos;

g. Troque as senhas de acesso das contas bancárias, redes sociais, e-mails e aplicativos;

h. Avise aos amigos e familiares que você foi vítima de golpe, principalmente se a fraude foi a de perfil hackeado ou clonado;

i. Acompanhe o extrato bancário para detectar transações suspeitas e avise o banco;

j. Também é indicado cancelar cartões de crédito para que criminosos não realizem transações;

k. Guarde ou salve comprovantes, imagens de telas, fotos, e-mails, mensagens suspeitas e quaisquer outros dados que possam ajudar a comprovar a fraude e, também, a encontrar os suspeitos.

Em caso de dúvidas ou não sendo solucionado a fraude, procure um advogado de sua confiança para que ele de posse dessas informações consiga lhe auxiliar.

O QUE FAZER SE TIVER SOFRIDO ALGUM DESSES GOLPES

O objetivo desta cartilha é instruir e proteger os consumidores não apenas a se prevenirem dos golpes aqui ilustrados, mas também que saibam o que fazer em caso de serem vítimas, pois a criatividade dos golpistas não tem limite.

As fraudes e os golpes financeiros mudam todo dia, portanto a melhor forma de prevenção é se manter informado. A cartilha já explicou como reconhecer e prevenir a ação dos golpistas, e agora vamos lhe ajudar como tentar reverter a situação caso seja lesado.

O QUE FAZER SE TIVER SOFRIDO ALGUM DESSES GOLPES

GOLPES DO PIX

Nos casos de sofrer o **Golpe do PIX**, nas modalidades aqui descritas, a vítima deverá:

- Fazer um Boletim de Ocorrência (até mesmo online) – em Mato Grosso Temos a Delegacia Especializada de Repressão a Crimes Informáticos;

- Avisar o mais rápido possível sua instituição financeira sobre a fraude para que o banco comunique com o banco que recebeu o dinheiro e tente bloqueá-lo, consequentemente será gerado um protocolo interno;

- Se o banco recebeu o dinheiro e não deu nenhuma resposta a vítima a mesma deverá abrir uma reclamação junto ao Bacen, assim como junto ao PROCON, ou consumidor.gov.br.

O QUE FAZER SE TIVER SOFRIDO ALGUM DESSES GOLPES

FRAUDE DE CARTÃO OU O GOLPE DO MOTOBOY

No caso de ter ocorrido a **Fraude de Cartão ou o Golpe do Motoboy** a vítima deverá:

- Avisar imediatamente a instituição financeira após a fraude;

- Fazer um Boletim de Ocorrência;

- Pedir o ressarcimento, de preferência por meio de documento formal por escrito, podendo ser realizado via canais oficiais, como por exemplo o consumidor.gov.br, ou o PROCON.

O QUE FAZER SE TIVER SOFRIDO ALGUM DESSES GOLPES

GOLPE DA MÃO FANTASMA

No caso de ter ocorrido o **Golpe da mão fantasma**, a vítima deverá:

- Interromper a comunicação do smartphone ou do computador/ notebook imediatamente, ou seja, desligue a internet, desative o Wi-Fi, em caso de celular, desligue-o e tire o chip da operadora;

- Trocar as senhas dos apps que você tiver instalado no celular.

- Se houve gastos no cartão de crédito, cancele-o imediatamente, entre em contato com a operadora e anote o protocolo, o horário de atendimento e o atendente;

- Entrar em contato com o banco de um outro aparelho telefônico para saber o que de fato aconteceu mesmo com sua conta, ou seja, para saber qual tamanho do prejuízo.

- Registrar imediatamente um Boletim de ocorrência e se atingiu a sua conta bancária, entre em contato com a instituição financeira, pedindo o estorno e o bloqueio imediato da conta e todas as relações.

O QUE FAZER SE TIVER SOFRIDO ALGUM DESSES GOLPES

GOLPE DO BOLETO FALSO

No caso de ter sofrido o **Golpe do Boleto Falso,** a vítima deverá:

- Denunciar e bloquear o perfil falso no app do WhatsApp, ou o site ou aplicativo utilizado para realizar a operação;

- Registrar um Boletim de Ocorrência e entre em contato com o estabelecimento e com a instituição financeira, objetivando o estorno da operação financeira, a fim de impedir que os fraudadores levantem o referido dinheiro.

O QUE FAZER SE TIVER SOFRIDO ALGUM DESSES GOLPES

GOLPE DO PHISING OU SMISHING BANCÁRIO

No caso de ter sofrido o **Golpe do Phising ou SMishing bancário**, a vítima deverá:

- Entrar em contato com delegacia de crimes virtuais e registrar um boletim de ocorrência;

- Desconectar seus dispositivos e altere suas senhas;

- Tenha sempre um backup disponível/ atualizado.

O QUE FAZER SE TIVER SOFRIDO ALGUM DESSES GOLPES

GOLPE DA FALSA CENTRAL DE ATENDIMENTO

No caso de ter sofrido o **Golpe da falsa central de atendimento**, a vítima deverá:

- Comunicar imediatamente seu banco por meio dos canais oficiais de atendimento;

- Fazer um boletim de ocorrência;

O QUE FAZER SE TIVER SOFRIDO ALGUM DESSES GOLPES

GOLPE DO FALSO LEILÃO

No caso de ter sofrido o **Golpe do Falso Leilão**, a vítima deverá:

- Informar sobre o golpe ao banco e solicitar o bloqueio da operação fraudulenta;

- Fazer boletim de ocorrência.

- Ligar para o banco que recebeu o crédito, informar sobre o ocorrido e pedir o bloqueio da operação.

O QUE FAZER SE TIVER SOFRIDO ALGUM DESSES GOLPES

GOLPE NO WHATSAPP

No caso de ter sofrido o **Golpe no WhatsApp**, a vítima deverá:

- O primeiro passo é avisar aos contatos, amigos e familiares pelas redes sociais ou outros meios possíveis. Evitando assim que seus contatos possam fazer transferências ou depósitos para os golpistas.

- Desconectar sua conta no aplicativo e ative novamente;

- No caso de usar WhatsApp Web/ Desktop, desconecte-o também.

- Uma boa dica também é desativar a visualização da sua foto de perfil do WhatsApp para que apenas pessoas que estão registradas na sua agenda como contato tenham acesso a foto.

O QUE FAZER SE TIVER SOFRIDO ALGUM DESSES GOLPES

GOLPE DA TROCA DE CARTÃO

No caso de ter sofrido o **Golpe da Troca de Cartão**, a vítima deverá:

- Bloquear o cartão fraudado;
- Fazer um Boletim de Ocorrência;
- Formalizar contestação administrativa no banco responsável pelo cartão pleiteando ressarcir o prejuízo.

O QUE FAZER SE TIVER SOFRIDO ALGUM DESSES GOLPES

GOLPE SITE, LINK OU PERFIL/PÁGINA DE REDE SOCIAL

No caso de ter sofrido o **Golpe Site, Link ou Perfil/Página de Rede Social Falsa das Instituições Bancárias**, a vítima deverá:

- Denunciar os perfis falsos;
- Fazer um Boletim de Ocorrência;
- A vítima busque o máximo de provas sobre a atuação indevida.

O QUE FAZER SE TIVER SOFRIDO ALGUM DESSES GOLPES

GOLPE DO FALSO PROTESTO

No caso de ter sofrido o **Golpe do falso protesto**, a vítima deverá:

- Fazer um Boletim de Ocorrência;
- Abrir reclamação junto a instituição financeira destinatária para que esta possa tentar bloquear a operação realizada;
- Efetivar reclamação junto a instituição financeira que originou a operação.

O QUE FAZER SE TIVER SOFRIDO ALGUM DESSES GOLPES

GOLPE DO DEPÓSITO PRÉVIO PARA LIBERAÇÃO DE EMPRÉSTIMO

No caso de ter sofrido o **Golpe do depósito prévio para liberação de empréstimo**, a vítima deverá:

- Fazer um boletim de ocorrência;
- Poderá a vítima solicitar a devolução na esfera cível de quem recebeu o dinheiro, com amparo na esfera criminal por estelionato.

Caso ocorra qualquer uma dessas fraudes, é imprescindível que a vítima contrate um advogado especialista, de sua confiança, para entender as providências que deverá tomar e as medidas judiciais que porventura sejam cabíveis.