CRIMES VIRTUAIS

COMO SE PREVENIR?

CONSELHO MUNICIPAL DE PROTEÇÃO E DEFESA DO CONSUMIDOR

PREFEITURA PARÁ DE MINAS

PROCON PARÁ DE MINAS

ORDEM DOS ADVOGADOS DO BRASIL

Comissão de Defesa do Consumidor

PARÁ DE MINAS / MG

VOCÊ SABE O QUE SÃO CRIMES VIRTUAIS?

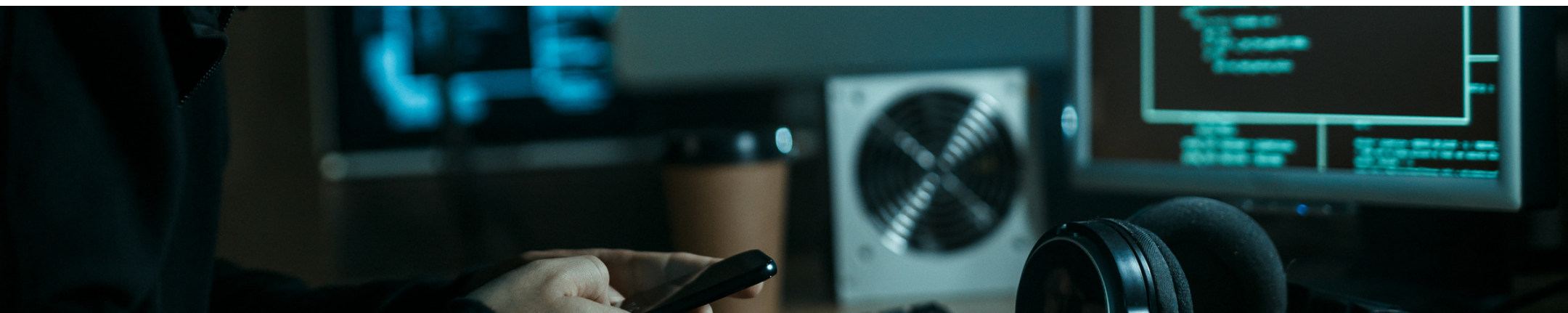
A tecnologia trouxe vantagens de acesso a informações, praticidades e ganho de tempo no nosso dia a dia. Em contrapartida, seu uso também trouxe inúmeros riscos. Em razão disso, é compreensível que muitas pessoas tenham receio de utilizar a tecnologia para realizar as tarefas do cotidiano, sobretudo quando envolve transações bancárias e compras na on-line.

Porém, com a crescente demanda por interações on-line, o dever de cuidado dos cidadãos tem diminuído, abrindo espaço para pessoas mal intencionadas praticarem uma gama de crimes virtuais.

Infelizmente, milhares de pessoas são vítimas dos mais variados golpes em ambientes virtuais, como, por exemplo: clonagem de aplicativos, extorsões e sequestros de dados.

Com o aumento de casos em nossa cidade, o Procon de Pará de Minas em parceria com a Comissão de Defesa do Consumidor da 18ª Subseção da OAB, elaboraram a presente cartilha com dicas de segurança contra golpes virtuais e presenciais, com o objetivo de promover uma cultura de segurança coletiva e prevenir a população contra fraudes.

IMPORTANTE RESSALTAR QUE NA OCORRÊNCIA DE CRIMES VIRTUAIS A COMPETENCIA DE SUA INVESTIGAÇÃO E PUNIÇÃO COMPETE AS FORÇAS POLICIAIS E AO PODER JUDICIÁRIO. AOS ÓRGÃOS DE DEFESA DO CONSUMIDOR CABE APENAS ORIENTAÇÃO AOS CONSUMIDORES.



PRINCIPAIS CRIMES VISTOS EM PARÁ DE MINAS

1 - GOLPE DO PIX ONLINE:

O chamado “Pix on-line”, constitui em mensagens encaminhadas para grupos de WhatsApp com ofertas de transferências diretamente para a conta, cartões de crédito desbloqueado, pagamento de boletos com descontos no valor devido e notas fiscaiss fakes.

O Código de Defesa do Consumidor, em seu art. 4º, III, diz ser pressuposto de toda relação de consumo a boa-fé das partes. Assim, o consumidor que contrata esses serviços já sabendo das irregularidades e no intuito de obter vantagem, viola a boa-fé e pode incorrer na prática de crime contra a ordem tributária (arts. 1º e 2º da Lei nº 8.137/1990), pois quem, de qualquer modo concorre para os crimes definidos nesta lei, incide nas penas a estes cominadas, na medida de sua culpabilidade (art. 11).

Assim, recomendamos para que não se utilizem desses serviços e que o CDC não socorre os consumidores que tiverem prejuízos nesta situação. Na dúvida, procurem a Polícia.

MECANISMOS DE SEGURANÇA:

Há duas ferramentas de segurança para transações bancárias que podem ser utilizadas para reaver o valor indevidamente transferido: o Bloqueio Cautelar (BC) e o Mecanismo Especial de Devolução (MED).

Segundo o Banco Central, o Bloqueio Cautelar pode ser solicitado junto à instituição bancária no caso de suspeita de fraude. Essa medida permitirá que no ato do crédito na conta, a instituição efetue um bloqueio preventivo dos recursos por até 72 horas. A opção vai possibilitar que a instituição realize uma análise mais detalhada da operação, aumentando a probabilidade de recuperação dos recursos pelos usuários vítimas de algum golpe.

Já o Mecanismo Especial de Devolução (MED) serve para o caso quando o usuário faz um Pix e em seguida se dá conta de que foi vítima de um golpe. Nesse tipo de situação, é preciso registrar um boletim de ocorrência e avisar imediatamente a instituição pelo canal de atendimento oficial, como SAC ou Ouvidoria. No ambiente Pix nos aplicativos dos bancos, há um link direto para o canal a ser utilizado para registrar a reclamação.

Após o bloqueio, e caso a fraude se comprove, a instituição de destino da operação poderá devolver os recursos para o usuário (vítima).

2 - CLONAGEM DO WHATSAPP:

Através de uma ligação telefônica ou mensagem de texto, o falsário se passa por representante de um site promocional, site de compras ou acaba enviando falsos convites para eventos badalados. Assim, convence o usuário a informar, via WhatsApp, os seis números que lhe foram enviados por SMS. Após obter essa informação, o golpista consegue clonar o aplicativo de mensagens WhatsApp.

DICAS DE PREVENÇÃO:

• Não compartilhar qualquer código ou senha com desconhecidos, sobretudo, via aplicativos de mensagens;
• Ativar a função “Verificação em duas etapas” no WhatsApp;
• No menu de três pontos, clique em “Configurações”, busque “Conta” e então escolha “Verificação/Confirmação em duas etapas”;
• Pressione “Ativar” e crie uma senha de seis dígitos para a conta do WhatsApp;
• Confirme e em seguida disponibilize um endereço de e-mail válido para o caso de esquecer o código;
• Clique em “Avançar” e confirme seu endereço de e-mail, em “Salvar”;
• Não compartilhar informações pessoais através de aplicativos de mensagens;
• Alertar imediatamente os contatos sobre a clonagem do aplicativo WhatsApp, caso ocorra, a fim de evitar o golpe;
• No caso de ser surpreendido com pedido de ajuda financeira de algum contato do WhatsApp, efetuar ligação telefônica para confirmar a real necessidade e nunca proceder de imediato com a transferência de dinheiro sem ter a devida comprovação da origem e destino.

3 – CORREÇÃO DE ERRO NO APLICATIVO DO BANCO:

A vítima recebe um SMS supostamente da instituição financeira que possui conta bancária com um link para atualização do aplicativo ou *login*. Logo após recebe uma ligação solicitando a instalação de aplicativos desconhecidos. O golpista pede para que a vítima acesse o link para conseguir atualizar o aplicativo.

Ao clicar no link, informações pessoais são obtidas pelos criminosos, efetivando o golpe.

No caso da instalação do aplicativo desconhecido a vítima pode dar acesso irrestrito do seu aparelho para os golpistas e esses realizam operações bancárias se passando pela vítima.

DICAS DE PREVENÇÃO:

- As instituições financeiras alertam que não enviam nenhum tipo de SMS ou entram em contato via telefone para regularizar o uso dos aplicativos;
- Não fornecer dados pessoais através de ligação ou mensagem;
- Não acessar links duvidosos ou e-mails suspeitos;
- Ativar o mecanismo de verificação em duas etapas do aplicativo de mensagens;
- Nunca realizar a instalação de aplicativos desconhecidos em seu aparelho eletrônico quando foi solicitado por ligações de pessoas desconhecidas.

4 -CADASTRO DA CHAVE DO PIX:

O criminoso envia links falsos por meio de aplicativos de mensagens, e-mail ou redes sociais, fazendo se passar por instituições bancárias, solicitando à vítima a realização de um suposto cadastro de sua chave PIX. O golpe prossegue quando os links levam a sites falsos de bancos ou à instalação de aplicativos maliciosos, que roubam dados pessoais e financeiros. O objetivo é pegar senhas bancárias ou números de cartões de crédito, entre outras informações confidenciais.

DICAS DE PREVENÇÃO:

• As instituições financeiras alertam que não enviam nenhum tipo de SMS ou entram em contato via telefone para regularizar o uso dos aplicativos;
• Não fornecer dados pessoais através de ligação ou mensagem;
• Não acessar links duvidosos ou e-mails suspeitos;
• Ativar o mecanismo de verificação em duas etapas do aplicativo de mensagens;
• Nunca realizar a instalação de aplicativos desconhecidos em seu aparelho eletrônico quando foi solicitado por ligações de pessoas desconhecidas.

5 – BOLETOS FALSOS:

O criminoso consegue a informação de que a vítima paga determinada dívida através de boleto bancário e emite um boleto falso com dados que não correspondem aos do real destinatário, mas sim de um falsário.

DICAS DE PREVENÇÃO:

• Sempre emitir os boletos no site oficial do banco ou do credor que está fazendo a cobrança;
• Não acessar sites de recálculo de boleto atrasado, em geral são falsos;
• Não acessar links duvidosos ou e-mails suspeitos;
• Antes de efetuar o pagamento, verificar se os três primeiros números da sequência correspondem ao código do banco que emitiu o boleto;

• Conferir se os dados do beneficiário ou da pessoa que vai receber o dinheiro estão corretos;
• Verificar se o código de barras que fica na região superior do documento é idêntico ao que aparece na parte inferior.

6 – SITES FRAUDULENTOS:

O estelionatário envia links por e-mail ou por aplicativos de mensagens e que são páginas praticamente idênticas às de grandes lojas online. O consumidor será induzido a acreditar que está realizando a compra, mas não receberá o produto e pior, não terá para quem processar ou como resgatar o valor pago.

DICAS DE PREVENÇÃO:

• Não acessar sites, links duvidosos ou e-mails suspeitos;
• Ter cuidado com propagandas recebidas que possam se caracterizar como spam;
• Manter antivírus e firewall atualizados;
• Realizar o pagamento em compras online através do cartão de crédito e evitar boleto ou PIX, pois a aquisição de produtos e serviços pelo cartão de crédito facilita o cancelamento da compra junto a administradora do cartão.

7 - VALE PRESENTES:

O criminoso envia um link oferecendo vale presentes falsos, em geral de grandes redes de supermercados ou de lojas conhecidas. Ao clicar no link e passar suas informações pessoais a vítima cai no golpe.

DICAS DE PREVENÇÃO:

- Desconfiar de promoções oferecidas através de mensagens;
- Não acessar sites, links duvidosos ou e-mails suspeitos;
- Antes de clicar em qualquer link, procurar saber em fontes oficiais, se a promoção realmente existe;
- Manter antivírus e firewall atualizados.

8 - EMPRÉSTIMO CONSIGNADO:

O criminoso deposita indevidamente uma quantia na conta da vítima, graças a algum cadastro realizado anteriormente em alguma instituição financeira ou correspondente bancário, o que, em muitos casos, possibilita o acesso à senha e login. Nos meses subsequentes são realizados descontos na conta ou no cartão de crédito da vítima referente ao empréstimo irregular.

DICAS DE PREVENÇÃO:

- Procurar sua instituição bancária no caso de qualquer quantia de origem duvidosa depositada em sua conta;
- Não permitir que pessoas estranhas preencham seus cadastros ou tenham o acesso de suas senhas e logins.

9 - FALSO EMPRÉSTIMO:

:

Os criminosos entram em contato diretamente por telefone, oferecendo condições especiais de empréstimo. Ao longo da conversa, o criminoso já possui valores fechados para cada parcela e solicita o pagamento de taxas antecipadas para liberação do valor em conta. Ao concordar com o empréstimo e realizar o pagamento, o consumidor é enganado e não consegue reaver o seu dinheiro. Aqui, os golpistas informam ao consumidor que para ter o seu empréstimo aprovado, ele precisa pagar antecipadamente o valor referente ao IOF (Imposto sobre Operações Financeiras) ou outra taxa do contrato.

O consumidor então antecipa o pagamento mas não recebe nenhum valor com o empréstimo.

DICAS DE PREVENÇÃO:

- Atentar que empresas certificadas pelo Banco Central não cobram taxas antecipadas para liberação de crédito, tampouco depósitos de valores em conta-corrente de pessoas físicas;
- Nunca depositar quaisquer quantias em contas desconhecidas;
- Desconfiar se estiver negativado e as condições oferta das para empréstimo forem muito atraentes.

10 - AÇÃO JUDICIAL DE COBRANÇA DE DÍVIDA:

O criminoso entra em contato com a vítima, normalmente mostrando algum documento com timbre falso do Tribunal de Justiça ou escritório de advocacia, informando que ela tem um débito junto a determinada empresa, loja ou instituição. Informa que o débito está sendo cobrado judicialmente e que a penhora de bens já foi decretada pelo juiz. O golpista pressiona a vítima a realizar pagamento de qualquer quantia para evitar a penhora de bens.

DICAS DE PREVENÇÃO:

- Não fornecer dados pessoais. Assuntos de caráter financeiro devem ser tratados, de preferência, pessoalmente;
- Entre em contato com a instituição, empresa ou loja que supostamente seria a responsável pela cobrança para verificar a existência do débito, em caso de dúvida;
- A prática judicial não prevê ligações telefônicas informando quanto ao êxito das ações.

11 - PIRÂMIDE FINANCEIRA:

A vítima é apresentada a um investimento com ganhos fáceis e extremamente tentadores. O golpe consiste no recrutamento de novos membros para o grupo. Um investidor indica um novo membro que ficará no nível abaixo dele, por sua vez, este integrante tem a meta de chamar mais pessoas para ocupar o de grau abaixo. Em determinado momento, a estrutura do grupo não se sustenta em razão da quantidade de pessoas e os que entram por último, em geral, acabam no prejuízo.

DICAS DE PREVENÇÃO:

- **Buscar formas confiáveis de investir dinheiro;**
- **Desconfiar de propostas financeiras com ganhos fáceis;**
- **Observar que a pirâmide financeira configura crime contra a economia popular.**

CONSIDERAÇÕES FINAIS

Este texto informativo destacou 11 estratégias utilizadas por criminosos que se aproveitam da boa-fé das pessoas para obterem recursos de forma fraudulenta, gerando sérios prejuízos às vítimas. Há ainda inúmeras modalidades além destas apresentadas, que são algumas das mais praticadas atualmente. Sendo assim, pontuamos ações de prevenção e segurança que auxiliam na blindagem contra fraudes virtuais de qualquer espécie:

A) Quando for realizar a aquisição de produtos ou serviços em lojas virtuais, confira sempre o site do "RECLAME AQUI", "PROCON" e "TRIBUNAL DE JUSTIÇA" para saber se existem reclamações recorrentes de outros consumidores contra essa empresa/loja.

B) Não acessar e-mails desconhecidos ou links suspeitos, uma vez que correspondem, em sua maioria, à porta de entrada para os criminosos terem acesso a dados e até mesmo senhas pessoais.

C) Não aceitar ajuda de estranhos em bancos ou casas lotéricas. O aconselhável é sempre se dirigir a algum funcionário do estabelecimento financeiro e se certifique que esteja identificado com crachá do banco. Na dúvida, peça algum parente para que o acompanhe junto ao banco no dia do pagamento, especialmente idosos.

D) Não fornecer dados pessoais por mensagens de texto, aplicativos de mensagens ou ligação telefônica para estranhos. Tente se dirigir pessoalmente à agência bancária em casos de dúvidas ou necessidades.

E) Não caia naquelas ligações recebidas que, de início, já pedem a confirmação do CPF e outros dados do consumidor. Peça que a pessoa que está ligando informe esses dados para que você possa confirmá-los e sempre pergunte onde foram coletados os seus dados.

F) Não existe dinheiro fácil, seja prudente ao tratar de assuntos financeiros.

G) Atenção com a documentação pessoal.

H) Nunca guardar cartão e senha no mesmo local. Além de evitar empregar senhas ligadas a dados pessoais como datas de aniversário, ou sequências fáceis como "1234" etc.

I) Manter a ferramenta de proteção digital atualizada (antivírus, firewall, etc.).

J) Manter ativado o mecanismo de ativação em duas etapas no aplicativo WhatsApp.

K) Não depositar valores em contas de estranhos.

A DICA MAIS IMPORTANTE É:

NO AMBIENTE VIRTUAL, FIQUE SEMPRE ALERTA. NUNCA REALIZE NADA POR IMPULSO. PARE, PENSE, CONFIRA.

FOI VÍTIMA DE UM GOLPE? VEJA ALGUMAS ATITUDES A SEREM TOMADAS IMEDIATAMENTE:

- **Comunicar o fato à instituição bancária e/ou à operadora do cartão da vítima;**

- **Trocar todas as senhas (e-mails, redes sociais, aplicativos) para ajudar a minimizar os danos;**

- **Reportar o golpe às autoridades competentes, principalmente à Polícia;**

- **Avisar a todos os familiares e amigos de sua rede de relacionamento, orientando que ignorem qualquer tentativa de contato estranho, sobretudo se solicitarem alguma quantia em dinheiro;**

- **Informar a operadora de telefonia celular bem como o suporte do aplicativo para que procedam com suas próprias medidas de segurança.**

CONTATOS PARA DENÚNCIAS:

POLÍCIA MILITAR 190

POLÍCIA CIVIL 181

MINISTÉRIO PÚBLICO MG (31) 3330-8100