FUNDO MUNICIPAL DE APOSENTADORIA E PENSÕES
ITAPIRA/SP

GOLPES CONTRA IDOSOS: OS 10 TIPOS MAIS COMUNS

Os golpes exploram a vulnerabilidade dos idosos e costumam aplicar a **engenharia social**: uma **técnica de manipulação para conseguir a confiança das pessoas e ter acesso a informações privadas**. Os golpes na internet também exploram a falta de familiaridade com certas tecnologias.

A Federação Brasileira de Bancos (Febraban) divulgou uma lista das 10 ações criminosas mais frequentes contra pessoas idosas. Confira a seguir quais são estes principais golpes e como identificá-los.

1. FALSA CENTRAL TELEFÔNICA

Um criminoso faz contato por telefone identificando-se como um funcionário do banco, alegando irregularidades na conta. Ele pode solicitar dados da vítima e pedir uma transferência para regularizar problemas na conta ou no cartão.

- **Fique alerta**: os bancos nunca solicitam por telefone, dados pessoais, senhas ou chaves de segurança, nem pedem transferências ou pagamentos. Ao receber uma ligação suspeita, a orientação é desligar e entrar em contato com o banco pelos canais oficiais.

2. FALSO EMPRÉSTIMO CONSIGNADO

O fraudador oferece por telefone, um **empréstimo consignado** ou uma **portabilidade** com boas condições, passando-se por um funcionário de uma instituição financeira. Para fechar a falsa proposta, solicita dados pessoais e pede um depósito bancário para cobrir as taxas de cadastro ou como adiantamento de parcela.

- **Fique alerta**: de acordo com a Febraban, não existe nenhum empréstimo que exija pagamento antecipado, seja de taxas ou de parcela. Nunca deposite dinheiro para alguém com a finalidade de garantir um negócio.

3. AJUDA NO CAIXA ELETRÔNICO

Ocorre quando o cliente está usando um terminal de autoatendimento e o criminoso oferece ajuda para fazer a transação. Um dos golpes é conferir a senha e trocar o cartão da vítima por um falso.

● **Fique alerta**: ao usar o caixa eletrônico, aceite ajuda apenas de funcionários do banco, devidamente identificados.

4. FALSO PRESENTE DE ANIVERSÁRIO

O criminoso, que já teve acesso aos dados e à data de aniversário da vítima, entra em contato avisando que tem um presente ou um brinde para entregar pessoalmente. Ao chegar com flores ou chocolate, pede um pagamento de taxa de entrega, feito no cartão. Com o visor da **maquininha** danificado ou encoberto, a vítima acaba digitando a senha no campo do valor da compra, revelando o código secreto ao criminoso.

● **Fique alerta**: tenha cuidado ao preencher seus **dados pessoais** em cadastros na internet e nunca aceite presentes sem saber quem enviou. Outra dica é nunca fazer pagamentos em maquininhas com o visor danificado, que impeça a visualização do valor.

5. VENDAS FALSAS

Envio de links com promoções por e-mails, SMS ou mensagens de celular. O endereço leva a uma página falsa que simula uma loja virtual, e os criminosos ficam com o valor da compra.

● **Fique alerta**: desconfie da oferta de produtos muito mais baratos que os vendidos pela concorrência. Além disso, não faça compras online em endereços virtuais recebidos por mensagem – mesmo que se pareça um site conhecido.

6. GOLPE DO WHATSAPP

O golpista tenta cadastrar o WhatsApp da vítima no seu aparelho. Este tipo de operação exige um código de segurança, que é enviado pelo app por SMS. Ao

enviar uma mensagem de WhatsApp para a vítima fingindo ser de um serviço de atendimento ao consumidor, o criminoso solicita o código recebido por SMS, alegando ser necessário para atualizar o cadastro na falsa empresa. Com esta informação, é possível clonar o WhatsApp da vítima.

- **Fique alerta**: para evitar a possível clonagem do WhatsApp, habilite no aplicativo a opção "Verificação em duas etapas" para cadastrar uma senha que será solicitada periodicamente. Nunca compartilhe essa senha com outras pessoas.

7. *PHISHING* (PESCARIA DIGITAL)

O ***phishing*** é uma maneira de conseguir dados pessoais da vítima. Normalmente ocorre pelo envio de mensagens e e-mails com um link suspeito. Esse endereço virtual pode solicitar o compartilhamento de dados ou simplesmente instalar um vírus capaz de roubar informações.

- **Fique alerta**: nunca abra links que chegam por mensagens e tenha sempre antivírus instalado no computador e no celular.

8. FALSO MOTOBOY

A vítima recebe a ligação de um criminoso se passando por funcionário do banco, informando que o **cartão de crédito foi clonado**. Ele solicita que uma nova senha seja digitada no telefone, que o cartão seja cortado ao meio e avisa que, por segurança, um motoboy irá buscar o cartão para perícia. Como o chip continua funcionando quando o cartão é cortado ao meio, os criminosos conseguem realizar operações financeiras.

- **Fique alerta**: nenhum banco pede de volta o cartão ou vai retirá-lo na casa dos clientes.

9. TROCA DE CARTÃO

Ao se passar por vendedores, golpistas observam a senha quando a vítima faz um pagamento na maquininha, e depois devolvem um cartão trocado. Dessa forma, ficam com o cartão e a senha da vítima.

- **Fique alerta**: sempre confira o seu cartão ao guardar de volta na carteira e, de preferência, não entregue a outra pessoa ao fazer uma compra.

10. FALSO SEQUESTRO

A vítima recebe uma ligação e do outro lado uma pessoa simula uma voz de choro, chamando pela mãe ou pelo pai, dizendo que foi sequestrada. Outro criminoso entra na linha e exige um dinheiro para o resgate do falso sequestro.

- **Fique alerta**: sempre desconfie desse tipo de ligação e nunca fale o nome de uma pessoa que poderia ter sido sequestrada. Se for possível, ligue imediatamente para este familiar, de outro telefone.

CAÍ EM UM GOLPE, O QUE FAZER?

Para proteger os idosos desses golpes, **é essencial que eles sejam informados sobre os diferentes tipos de fraudes e estejam cientes das medidas preventivas**. Família, amigos e cuidadores devem estar atentos a mudanças no comportamento financeiro, recebimento de ligações suspeitas ou compartilhamento de informações pessoais com desconhecidos. Se a pessoa idosa ou a família constatar que houve um golpe financeiro, é importante seguir estas orientações:

1. ENTRE EM CONTATO COM O BANCO

Avise imediatamente o banco para que sejam tomadas medidas de segurança, como bloqueio do aplicativo e da senha de acesso.

2. FAÇA UM BOLETIM DE OCORRÊNCIA

O crime deve ser denunciado em uma delegacia online por meio de um boletim de ocorrência.

3. DENUNCIE AO GOVERNO

O Disque 100 é um canal disponível para essas denúncias no Ministério da Cidadania e Direitos Humanos. O serviço de atendimento é gratuito, sigiloso e funciona 24 horas por dia, todos os dias da semana. Após o registro, as denúncias são encaminhadas às autoridades competentes para investigação.

SEIS SINAIS DE GOLPE DIGITAL

Em 2023, os golpes digitais foram responsáveis por fazer os brasileiros perderem cerca de R$1,1 bilhão, conforme mostrou um estudo de mercado inédito realizado pela OLX, uma das maiores plataformas de compra e venda online do país. Novo número de celular, golpe do pix, falsa central de atendimento, pagamento em aberto, invasão de conta. Tem de tudo por aí, mas a lógica é sempre a mesma: para conquistar o que querem, os golpistas agem de forma a induzir suas vítimas a executar alguma ação ou tomar decisões no impulso para roubar dinheiro ou informações sensíveis.

1. PROPOSTA QUE PARECE BOA DEMAIS PARA SER VERDADE

Todo mundo gosta de uma promoção e de aproveitar boas oportunidades para pagar menos por aquele produto tão desejado. E os golpistas sabem disso. Por isso, tiram proveito da vulnerabilidade dos consumidores para chamar a atenção com descontos imperdíveis – como itens de alto valor à venda por preços significativamente reduzidos. A dica, portanto, é desconfiar. Quando a proposta parece boa demais para ser verdade, algo deve estar errado. Assim, no ímpeto de querer fechar a compra, primeiro ligue o alerta.

2. PEDIDO DE URGÊNCIA E PRAZO LIMITADO

A urgência é um dos mais evidentes sinais de golpe digital. Os criminosos têm pressa e, por isso, forçam os consumidores a agir rapidamente, seja fechando uma compra naquele momento, seja enviando logo uma transferência de dinheiro. Propagandas que anunciam descontos que duram poucas horas ou itens se esgotando no estoque também costumam fazer parte da estratégia. A lógica é fazer com que a vítima não tenha tempo de pensar ou avaliar melhor a

situação. Isso acontece porque o tempo é crucial para os golpistas. Eles precisam agir rapidamente antes que sejam descobertos ou denunciados por outros consumidores – o que é muito comum em golpes que **clonam o telefone** de uma pessoa e mandam mensagem a seus contatos avisando sobre o novo número e pedindo dinheiro. Por isso, duvide sempre da urgência. No caso de pedidos de dinheiro pelo WhatsApp, não faça a transferência antes de averiguar quem está por trás daquele número. Se possível, ligue para a pessoa para confirmar se é ela ou mande mensagens fazendo perguntas para saber se as respostas estão corretas.

3. PEDIDOS DE SENHA E INFORMAÇÕES DESNECESSÁRIAS

Sempre desconfie de pessoas que entram em contato para pedir dados e informações que normalmente não são passadas a terceiros. Mesmo quando ela se identifica como representante de alguma empresa ou instituição, é cordial e simula transferências para outros atendentes. Bancos não ligam para pedir a senha do cartão, por exemplo. Essa informação não é solicitada nem pelos atendentes nas agências físicas, então não seriam exigidas à distância. O mesmo vale para outros dados pessoais, como CPF. O segredo aqui é não se desesperar. Em geral, os golpistas têm discurso pronto e tentam causar alarde ao fazer o alerta sobre uma movimentação suspeita na conta, o cartão clonado ou uma compra de alto valor no cartão de crédito em determinada loja, justificando o contato como um procedimento de segurança. Essa prática não existe. Na dúvida, nunca leve a conversa adiante. Desligue a chamada e, se for o caso, tente ligar para um número oficial daquela instituição.

4. ERROS DE PORTUGUÊS E DESIGN AMADOR NAS MENSAGENS ENVIADAS

Outro sinal de golpe digital são e-mails ou mensagens enviadas com erros óbvios de português ou design amador. Muitas vezes, isso é até proposital, pois é uma tática de enganar os filtros de spam. Por isso, esteja atento à substituição de letras por números de aparência semelhante ou alternância de outros alfabetos. Seja qual for o motivo dos erros de digitação, acenda o alerta assim que identificar qualquer coisa estranha.

5. EXIGÊNCIA DE PEQUENO PAGAMENTO

Outro truque favorito depois de fisgar a vítima é solicitar um pequeno pagamento, uma transferência para verificar o cartão ou o pagamento pelo registro em algum banco de dados. Sem ele, segundo os golpistas, não será possível receber a recompensa prometida. A quantia solicitada costuma ser pequena e insignificante diante da perspectiva de riquezas incalculáveis e pode até vir com garantia de recuperação em data posterior. Esse dinheiro é a primeira coisa a ser roubada, é claro. Não haverá prêmio, apenas a chance de perder ainda mais depois de compartilhar as informações de seu cartão de crédito com golpistas.

6. TENHA CUIDADO COM A MÁQUINA DE CARTÃO NAS COMPRAS PRESENCIAIS

Essa é para quem faz compras presenciais: o consumidor entrega o cartão a um vendedor para fazer um pagamento e ele se vira com a justificativa de que o sinal não está pegando. Acenda o alerta quando isso acontecer. Isso pode ser motivo para que ele troque seu cartão, tire fotos ou anote os dados. O número, o código de segurança e a validade podem ser usados facilmente para fazer compras na internet. Outra situação que pode acontecer são as máquinas com o visor quebrado. Isso pode ser motivo para o vendedor registrar um valor muito maior que o correto. Nessas horas, é importante ficar atento. Se não é possível visualizar, peça para trocar a máquina ou, então, espie o celular que costuma notificar os pagamentos realizados e pode confirmar o valor pago.