Guia Prático de Prevenção a Golpes

Confidencialidade do Documento: PÚBLICA
Sem restrição de divulgação.

Introdução

CAPÍTULO 1

A vida moderna, especialmente com o avanço da tecnologia e a facilidade proporcionada pela internet, trouxe inúmeras conveniências para o nosso dia a dia, desde transações bancárias até interações sociais e pesquisas. Contudo, essa mesma facilidade também abriu portas para **armadilhas que podem causar prejuízos financeiros, dificuldades de comunicação e riscos à proteção dos nossos dados e informações pessoais.**

É com o objetivo de fortalecer a sua segurança no ambiente digital e físico que preparamos este guia. Ele foi elaborado para todos os clientes da 2TM Participações S.A. e suas empresas controladas ("Grupo 2TM"), trazendo **hábitos simples e dicas de prevenção contra os principais golpes praticados na atualidade.**

Entendemos que a **sua segurança é uma prioridade**, e ao seguir as orientações aqui apresentadas, você estará mais preparado para se proteger contra tentativas de fraude.

Lembre-se de que a segurança das suas informações e da sua conta é uma responsabilidade compartilhada, e este material é uma ferramenta para te auxiliar nessa jornada de proteção.

02

Medidas essenciais para a sua segurança

CAPÍTULO 2

Para a sua segurança e a proteção de suas informações, o Grupo 2TM preparou uma série de hábitos e dicas importantes de segurança da informação para que você tenha uma melhor experiência no meio digital:

01 Não forneça informações pessoais ou de conta a qualquer pessoa.

02 Desconfie se você receber um e-mail ou SMS com links. Não clique no link.

03 Habilite a confirmação em duas etapas em seu aparelho celular e jamais envie códigos recebidos por SMS ou senhas para qualquer pessoa.

04 Sempre baixe aplicativos nas lojas oficiais, não baixe através de fontes duvidosas.

CAPÍTULO 2

05 Não forneça permissão para que aplicativos acessem informações confidenciais ou sensíveis em seu dispositivo, como senhas, fotos ou dados financeiros.

06 Confira sempre o destinatário no momento de realizar uma transferência bancária e não realize transferências para empresas e pessoas físicas desconhecidas.

07 Desconfie de mensagens ou ligações de números desconhecidos ou suspeitos.

08 Se você receber um boleto inesperado, confira todas as informações ali presentes, como banco de destino, valor, data de vencimento e demais dados.

09 Se você suspeitar de uma fraude ou tiver alguma dúvida sobre a sua segurança de sua conta bancária, entre em contato imediatamente com seu banco.

10 Não acredite em ofertas de emprego que chegam por desconhecidos pelo WhatsApp. As empresas possuem canais oficiais para envio de currículos e divulgação das suas vagas, como site ou mesmo a rede social profissional LinkedIn.

03

Tipos de Golpe

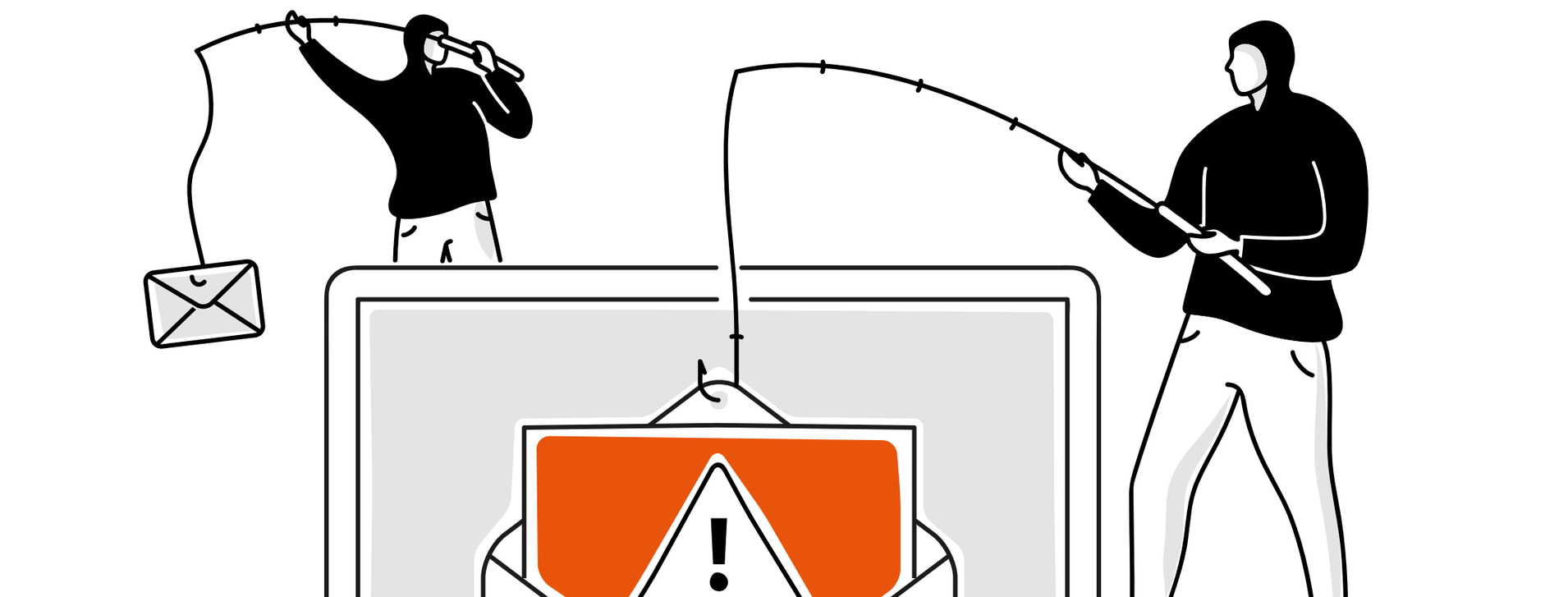
CAPÍTULO 3

3.1 Phishing

O que é Phishing?

Phishing é um tipo de fraude eletrônica onde criminosos tentam **enganar você para obter suas informações pessoais e financeiras, como senhas, dados do cartão de crédito, informações bancárias e até acesso às suas contas e investimentos.**

Eles fazem isso se passando por instituições confiáveis, como bancos, corretoras ou serviços digitais, geralmente enviando mensagens falsas por e-mail, SMS, WhatsApp ou redes sociais.



CAPÍTULO 3

Como acontece o Phishing?

Os criminosos criam mensagens muito parecidas com as reais, usando logotipos, linguagem formal e até remetentes falsificados. Essas mensagens contêm links para sites falsos (sites "clones") que imitam o visual de empresas.

Exemplos práticos:

- Você recebe um e-mail ou SMS dizendo que sua conta bancária foi bloqueada e precisa "verificar seus dados" urgentemente, com um link para um site falso parecido com o do seu banco.

- Você recebe uma mensagem no WhatsApp que oferece um investimento com retorno garantido e, para participar, pede que você clique em um link para preencher seus dados pessoais.

- Você recebe um anexo no e-mail que promete um boleto ou comprovante de pagamento, mas ao abrir, instala um vírus que captura suas senhas.

CAPÍTULO 3

Frequentemente essas mensagens usam senso de urgência, como “sua conta será bloqueada em 1 hora” ou “oferta exclusiva, só hoje”, para pressionar você a agir rápido sem pensar.

Os sites falsos frequentemente têm **URLs com erros de digitação ou caracteres estranhos**, por exemplo:

“mercadobiitcoin.com.br”
(com troca ou repetição de letras)

URLs com números ou símbolos estranhos:
“**123www**.exemplo.com” ou
“www.**me4i343d**.com/j34d”

CAPÍTULO 3

Como se prevenir?

01 Nunca clique em links suspeitos. Prefira acessar o site digitando o endereço diretamente no navegador.

02 Desconfie de mensagens com erros de português ou que criam urgência exagerada.

03 Não baixe anexos de remetentes desconhecidos ou não solicitados.

04 Sempre confirme a autenticidade da mensagem pelo canal oficial da empresa. Ligue para o atendimento oficial se tiver dúvida.

05 Use autenticação de dois fatores (2FA) sempre que possível nas suas contas bancárias e de investimentos.

06 Mantenha seu antivírus e sistema operacional atualizados.

07 Eduque-se e seus familiares sobre os golpes mais comuns, pois criminosos usam métodos parecidos para enganar pessoas de todas as idades.

CAPÍTULO 3

3.2 Golpe da Falsa Vaga de Emprego

O que é?

Esse golpe consiste na **oferta enganosa de uma vaga de emprego**, geralmente em empresas conhecidas e com salários atrativos, com o objetivo principal de coletar dados pessoais e financeiros das vítimas.

A vaga é falsa e serve apenas para os fraudadores roubarem informações importantes, que podem ser usadas para golpes financeiros.

CAPÍTULO 3

Como acontece?

Os criminosos entram em contato por WhatsApp, e-mail ou redes sociais, oferecendo uma vaga com condições aparentemente imperdíveis. Eles pedem que você faça um cadastro, enviando documentos pessoais, fotos, comprovantes e até assinatura digital. Em alguns casos também pedem um envio de dinheiro (antecipação de recursos) para vaga.

Exemplos práticos:

- Você recebe uma mensagem dizendo que foi pré-selecionado para uma vaga em uma grande empresa e deve enviar documentos para continuar o processo.

- O golpista solicita o envio de CPF, RG, comprovante de residência e, em alguns casos, pede assinatura digitalizada para “formalizar a contratação” e até mesmo envio de dinheiro, com a justificativa de antecipação de recursos.

- Com esses dados, os fraudadores podem abrir contas bancárias, solicitar cartões de crédito e fazer outras fraudes financeiras em seu nome.

CAPÍTULO 3

Como se prevenir?

01 Desconfie de vagas oferecidas por WhatsApp ou e-mail, principalmente se você não está buscando emprego no momento.

02 Nunca envie documentos pessoais ou assinaturas por canais não oficiais.

03 Candidatar-se somente através dos sites e redes oficiais das empresas.

04 O Grupo 2TM divulga vagas apenas no LinkedIn e na plataforma Gupy. Desconfie de qualquer oferta fora desses canais.

05 Bloqueie e denuncie contatos suspeitos imediatamente.

06 Em caso de dúvida, confirme diretamente com a empresa pelo canal oficial.

CAPÍTULO 3

3.3 Golpe da Central Telefônica Falsa

O que é?

Esse golpe ocorre quando criminosos usam **números falsificados para parecerem ligações oficiais** do banco. Eles se passam por funcionários tentando obter informações pessoais e senhas para acessar suas contas e aplicar fraudes.

CAPÍTULO 3

Como acontece?

Você recebe uma ligação de uma central telefônica que parece legítima, pois o número do telefone é idêntico ao do banco (número replicado, técnica chamada "spoofing").

O golpista se apresenta como funcionário do banco e confirma informações pessoais que já foram coletadas, muitas vezes pela internet ou redes sociais.

Para ganhar sua confiança, eles podem usar gravações verdadeiras de atendimentos anteriores.

Durante a ligação, pedem para você atualizar sistemas, fornecer senhas ou liberar o uso de equipamentos (como token ou app de segurança).

Também podem indicar sites falsos para você digitar seus dados bancários, roubando assim seu acesso.

CAPÍTULO 3

Como se prevenir?

01 Nunca informe ou digite sua senha, número do cartão ou dados da conta por telefone.

02 Não compartilhe sua senha de acesso ao banco com ninguém, nem por telefone.

03 Se receber uma ligação suspeita, desligue imediatamente. Depois entre em contato com o canal oficial do banco, de preferência escolhendo um canal diferente do que entrou em contato com você.

04 Não instale aplicativos indicados por ligações ou mensagens suspeitas. Se algum aplicativo foi instalado sem sua autorização, remova-o e busque ajuda do suporte técnico.

05 Baixe aplicativos somente de fontes oficiais (Google Play, App Store).

06 Verifique avaliações e reputação do aplicativo antes de instalar.

CAPÍTULO 3

Como se prevenir?

07 Nas configurações do seu dispositivo, bloqueie instalações de apliactivos de fontes desconhecidas.

08 Não conceda permissões para aplicativos acessarem dados confidenciais, como senhas, fotos ou informações financeiras.

CAPÍTULO 3

3.4 Golpe do Falso Atendimento pelo WhatsApp

O que é?

Nesse golpe, os criminosos se passam por atendente virtual da empresa, para **enganar clientes e obter acesso às suas contas de WhatsApp e dados pessoais**, podendo aplicar fraudes financeiras e golpes contra familiares e amigos da vítima.

CAPÍTULO 3

Como acontece?

Os golpistas entram em contato via mensagens ou ligações pelo WhatsApp, se passando por atendente virtual da empresa.

Alegam que houve um erro no sistema, oferecem serviços gratuitos ou pedem informações sigilosas, como número do cartão e senha.

Em seguida, solicitam que a vítima informe o código de verificação do WhatsApp enviado por SMS.

Com esse código, os criminosos acessam sua conta de WhatsApp, podendo ver suas conversas, contatos e grupos.

A partir daí, eles se passam por você para pedir dinheiro a familiares e amigos, através de mensagens falsas.

CAPÍTULO 3

Como se prevenir?

01 Desconfie sempre de mensagens e ligações que pedem informações pessoais ou códigos do WhatsApp.

02 Nunca informe códigos de verificação do WhatsApp para ninguém.

03 Verifique se o perfil da empresa no WhatsApp é oficial, com selo de verificação. Sempre clique no nome do contato para conferir os detalhes.

04 Se receber contato suspeito, bloqueie e denuncie o perfil imediatamente.

CAPÍTULO 3

3.5 Golpe do Falso Entregador

O que é?

Esse golpe consiste em uma **ligação falsa** onde o criminoso se passa por funcionário de empresas como bancos, **para convencer a vítima de que seu cartão foi clonado.** O objetivo é coletar dados e o próprio cartão para usar em fraudes.

CAPÍTULO 3

Como acontece?

O golpista liga para o cliente, afirmando que o cartão foi clonado e mostrando supostas compras que o cliente não fez.

Eles orientam o cliente a ligar para a Central de Atendimento para “resolver o problema”.

Quando o cliente tenta ligar, a ligação falsa continua, e o golpista mantém o contato, simulando ser o atendimento oficial.

Durante a conversa, solicitam dados pessoais e senha do cartão.

Após obter essas informações, pedem que o cliente corte o cartão ao meio e entregue para um motoboy que irá buscá-lo em casa.

Com o cartão e as informações, os criminosos podem realizar fraudes e saques indevidos.

CAPÍTULO 3

Como se prevenir?

01 Nunca entregue seu cartão a ninguém, mesmo que esteja cortado ou danificado.

02 Se receber esse tipo de ligação, desligue imediatamente e entre em contato com o canal oficial do banco, de preferência escolhendo um canal diferente do que entrou em contato com você.

03 Jamais forneça sua senha ou dados pessoais por telefone.

CAPÍTULO 3

3.6 Golpe da Maquininha com Visor Quebrado no Delivery

O que é?

Este golpe ocorre durante entregas de comida por delivery, onde o **criminoso utiliza uma maquininha de cartão com o visor quebrado ou danificado para cobrar um valor maior** do que o pedido original.

Como acontece?

No momento da entrega, o golpista apresenta a maquininha para que você faça o pagamento.

O visor da maquininha está quebrado ou danificado, dificultando a visualização do valor cobrado.

O valor que aparece na maquininha é maior do que o preço real do pedido.

Como você não consegue conferir o valor correto na hora, acaba aprovando uma cobrança maior.

CAPÍTULO 3

Como se prevenir?

01 Prefira realizar o pagamento diretamente pelo aplicativo oficial do serviço de delivery, evitando pagamentos em maquininhas físicas.

02 Sempre desconfie e cheque o valor cobrado antes de confirmar o pagamento.

03 Nunca aceite pagar em maquininhas com o visor quebrado ou danificado.

04 Ative o serviço de notificações via SMS ou aplicativo do banco para receber alertas imediatos de pagamentos realizados.

05 Caso perceba alguma cobrança indevida, entre em contato com seu banco imediatamente para contestar a transação.

CAPÍTULO 3

3.7 Golpe do Falso Cadastro de Chave Pix

O que é?

Nesse golpe, criminosos se passam por representantes de instituições financeiras para **enganar você e fazer com que cadastre sua chave Pix em sites falsos**.
O objetivo é roubar seus dados pessoais e financeiros.

CAPÍTULO 3

Como acontece?

Você recebe mensagens por e-mail, SMS ou WhatsApp supostamente de seu banco, solicitando que faça o cadastro ou atualização da sua chave Pix.

Os golpistas enviam links para sites falsos que imitam os canais oficiais do banco.

Ao acessar esses sites, você pode ser solicitado a informar dados pessoais, códigos de verificação enviados por SMS ou e-mail e até mesmo dados bancários.

Com essas informações, os criminosos podem acessar sua conta e realizar transações fraudulentas.

CAPÍTULO 3

Como se prevenir?

01 Nunca compartilhe códigos de verificação recebidos por SMS ou e-mail durante o cadastro das chaves Pix.

02 Se estiver inseguro em fornecer seus dados pessoais (CPF, telefone, e-mail) para receber pagamentos Pix, cadastre uma chave aleatória.

03 Desconfie de links recebidos por e-mail, SMS ou WhatsApp com pedidos para cadastramento ou atualização das chaves Pix.

04 Cadastre suas chaves somente pelos canais oficiais do banco (app, internet banking, site oficial).

05 Nunca faça transações a pedido de terceiros para supostos testes de suas chaves Pix.

06 Em caso de dúvidas, entre em contato diretamente com o banco pelo canal oficial.

CAPÍTULO 3

3.8 Golpe do Empréstimo Fraudulento

O que é?

Nesse golpe, o criminoso usa técnicas de engenharia social para **obter seus dados pessoais e financeiros** e, em seguida, **contrata um empréstimo em seu nome sem que você saiba**. Depois, tenta enganar você para que devolva o valor por meio de um Pix.

CAPÍTULO 3

Como acontece?

O golpista consegue suas informações pessoais e documentos, muitas vezes por meio de golpes ou vazamentos de dados.

Com esses dados, ele contrata um empréstimo fraudulento em seu nome, e o dinheiro é depositado na sua conta.

Logo após, o golpista entra em contato, alegando que o crédito foi um erro, e pede que você devolva o valor via Pix.

A vítima, acreditando no golpe, realiza a transferência e só depois percebe que caiu em uma fraude.

CAPÍTULO 3

Como se prevenir?

01 Sempre confirme se está falando com a empresa oficial. Desconfie de links enviados por mensagens, pois podem levar a sites falsos ou conter vírus.

02 Não forneça informações pessoais ou dados bancários por telefone, e-mail ou mensagens.

03 Os bancos nunca pedem sua senha ou dados bancários por e-mail ou telefone.

04 Se receber ligação ou mensagem suspeita de alguém se passando pelo banco, não forneça nenhuma informação. Desligue e entre em contato com o canal oficial do banco, de preferência escolhendo um canal diferente do que entrou em contato com você.

05 Ao ligar para o banco, use outro telefone para evitar que a linha esteja “presa” com o golpista.

06 Se quiser cancelar um empréstimo desconhecido, faça a solicitação diretamente com seu gerente ou pelos canais oficiais do banco.

CAPÍTULO 3

3.9 Golpe do Falso Boleto

O que é?

Esse golpe consiste na **alteração dos dados do boleto bancário**, de modo que o valor pago pela vítima seja transferido para uma conta controlada pelo golpista, e não para o beneficiário legítimo.

Como acontece?

O golpista altera informações importantes do boleto, como o número da conta e do banco beneficiário.

Isso pode acontecer tanto em boletos enviados fisicamente pelos Correios quanto em boletos digitais recebidos pela internet.

Quando a vítima realiza o pagamento, o dinheiro vai para a conta do criminoso, que pode movimentá-lo rapidamente.

CAPÍTULO 3

Como se prevenir?

01 Sempre confira atentamente as informações no boleto antes de pagar: valor, nome do beneficiário e código do banco.

02 Os três primeiros dígitos do código de barras indicam o banco emissor do boleto. Verifique se eles correspondem ao banco correto.

03 Se for emitir uma segunda via do boleto, confirme se o código do banco é o mesmo da via original. Caso seja diferente, não faça o pagamento.

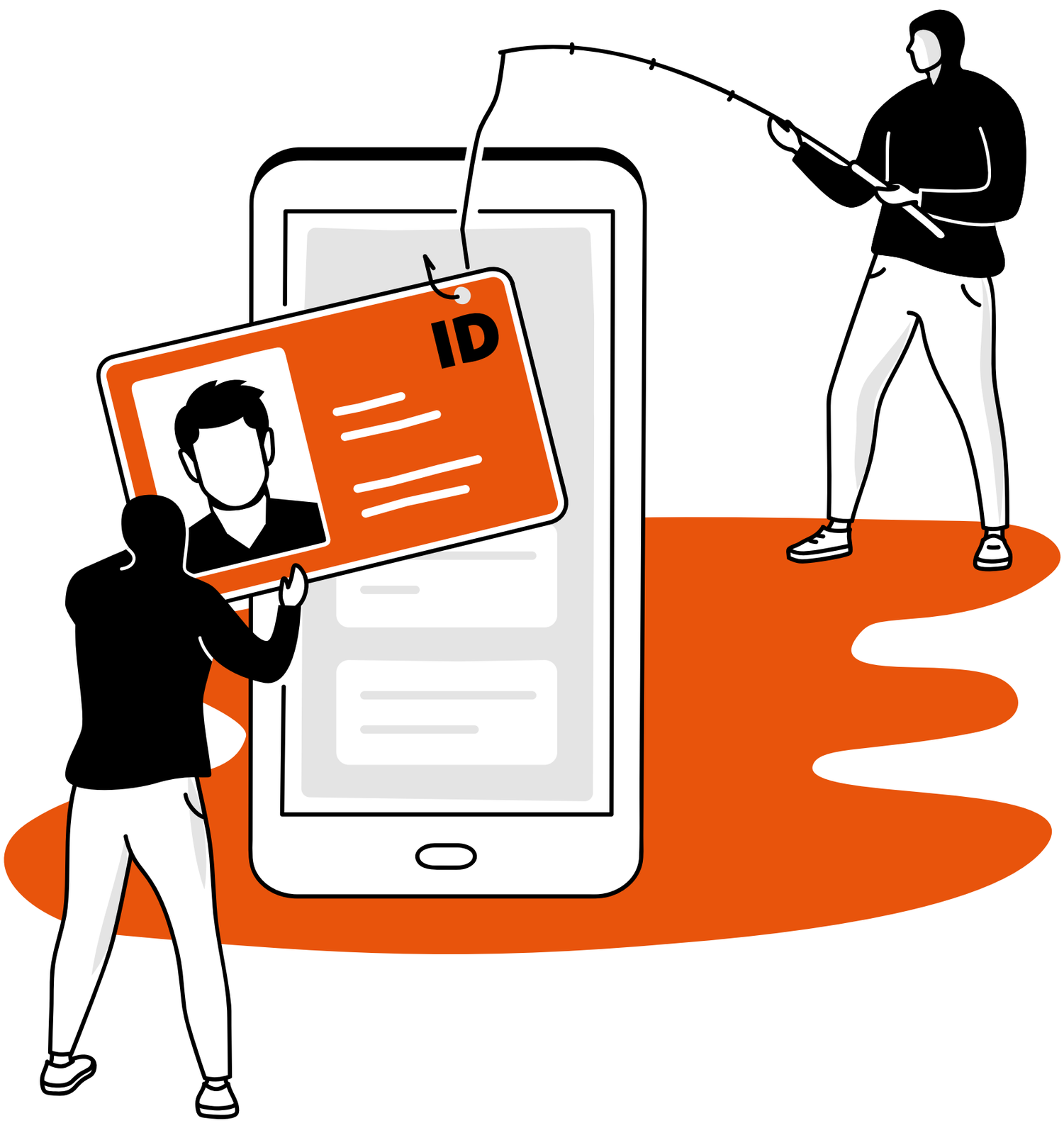
04 Prefira pagar boletos diretamente pelo site ou app oficial do banco, evitando copiar e colar códigos suspeitos.

05 Em caso de dúvida, entre em contato com a empresa emissora do boleto pelos canais oficiais para confirmar os dados.

3.10 Golpe da Oferta Falsa para Quitar Empréstimo

O que é?

Nesse golpe, o criminoso **liga para clientes que têm empréstimos consignados e oferece quitar a dívida por um valor inferior ao saldo real**, enganando a vítima para obter informações pessoais ou até mesmo dinheiro.



CAPÍTULO 3

Como acontece?

O golpista liga para o cliente, alegando ser do banco.

Oferece um valor para quitar o empréstimo consignado que é menor do que o saldo devido.

O objetivo é enganar o cliente para que ele forneça dados pessoais, informações bancárias ou realize pagamentos indevidos.

CAPÍTULO 3

Como se prevenir?

01 Sempre confirme se está falando com a empresa oficial antes de fornecer qualquer informação.

02 Desconfie de links recebidos por mensagens ou e-mails, pois podem levar a sites falsos ou conter vírus.

03 Nunca forneça suas informações pessoais, senhas ou dados bancários por telefone, e-mail ou redes sociais.

04 Os bancos nunca solicitam senha ou dados da conta por esses meios.

05 Não compartilhe dados pessoais em redes sociais para evitar exposição.

CAPÍTULO 3

Como se prevenir?

06 Se receber ligações ou mensagens suspeitas de números desconhecidos que dizem ser do banco, não forneça informações.

---

07 Desligue a ligação suspeita e, em seguida, ligue para os canais oficiais do banco, preferencialmente de outro telefone, para confirmar a veracidade da oferta.

---

07 Tenha cuidado, pois a linha onde recebeu a ligação pode estar “presa” pelo golpista, mantendo-o na linha.

CAPÍTULO 3

3.11 Golpe do Empréstimo Fácil com Pagamentos Antecipado

O que é?

Esse golpe consiste na **oferta de empréstimos com condições muito vantajosas**, que exigem o **pagamento antecipado de uma taxa**, comissão, seguro ou imposto. Após o pagamento, o criminoso desaparece sem liberar o crédito.

CAPÍTULO 3

Como acontece?

O golpista faz anúncios em sites, distribui folhetos na rua ou liga diretamente para clientes, oferecendo empréstimos com condições muito facilitadas.

Quando o cliente demonstra interesse, o golpista informa que é necessário pagar uma taxa, comissão, seguro ou imposto antes da liberação do valor.

Após o pagamento dessa “taxa” para a conta indicada, o golpista some, sem liberar o empréstimo.

CAPÍTULO 3

Como se prevenir?

01 Nunca faça transferências ou pagamentos antecipados para pessoas físicas ou empresas desconhecidas.

02 Nenhuma instituição financeira legítima solicita pagamento antecipado para liberar empréstimos.

03 Desconfie de ofertas de empréstimos com taxas muito baixas, sem avalista ou exigências incomuns.

04 Procure sempre contratar empréstimos diretamente pelos canais oficiais do banco ou instituições financeiras reconhecidas.

05 Em caso de dúvidas, consulte seu gerente ou o canal oficial do banco antes de fazer qualquer pagamento.

CAPÍTULO 3

3.12 Golpe do Cancelamento ou Substituição Falsa do Cartão

O que é?

Nesse golpe, o criminoso finge ser do banco e informa que seu **cartão será cancelado ou substituído**. O objetivo é fazer com que você forneça os dados do cartão e a senha para usar essas informações em fraudes.

CAPÍTULO 3

Como acontece?

O golpista liga para o cliente, dizendo que o cartão foi ou será cancelado.

Para “confirmar” ou “efetivar” o cancelamento/substituição, o cliente é transferido para um atendimento eletrônico.

Nesse atendimento, o cliente é orientado a digitar o número do cartão e a senha no telefone.

Um dispositivo grava os números digitados e envia essas informações ao golpista.

Com esses dados, o criminoso pode fazer saques, empréstimos e outras fraudes na conta da vítima.

CAPÍTULO 3

Como se prevenir?

01 Nunca informe ou digite os dados e a senha do seu cartão pelo telefone.

02 Os bancos jamais entram em contato solicitando número ou senha do cartão por telefone.

03 Se tiver dúvidas sobre qualquer ligação, entre em contato diretamente com a equipe oficial do banco pelos canais de atendimento.

CAPÍTULO 3

3.13 Golpe da Carteira no Chão

O que é?

O golpe da carteira no chão é uma abordagem criminosa usada para distrair e enganar a vítima, levando-a a um local onde **pode ser roubada ou ter seus dados utilizados para fraudes financeiras.**

CAPÍTULO 3

Como acontece?

O cliente sai do banco e duas mulheres jogam uma carteira no chão, esperando que o cliente veja e avise que a carteira caiu.

Como agradecimento, elas oferecem uma bonificação ou presente, ganhando a confiança da vítima.

Em seguida, levam a pessoa para um local isolado para roubá-la.

Caso o cliente carregue senhas anotadas junto com o cartão, os criminosos podem usar essas informações para contratar empréstimos pessoais e realizar outras fraudes em nome da vítima.

CAPÍTULO 3

Como se prevenir?

01 Nunca pare para conversar com estranhos em situações suspeitas.

02 Se deparar com algo no chão, ignore e siga seu caminho sem interagir.

03 Nunca anote suas senhas junto com o cartão ou em locais acessíveis.

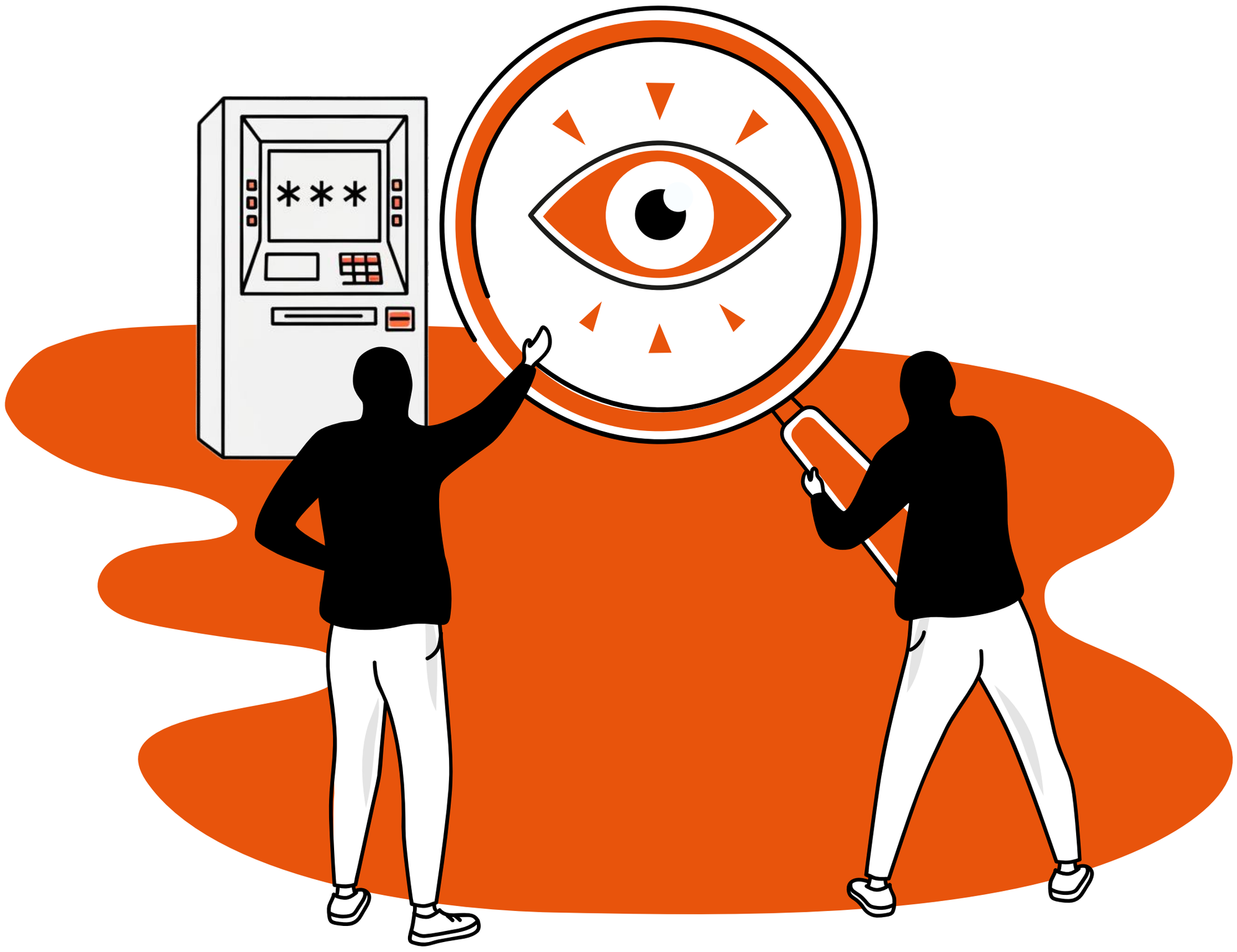
04 Tenha cuidado redobrado ao sair do banco ou em locais públicos.

CAPÍTULO 3

3.14 Golpe da Troca de Cartões

O que é?

O golpe da troca de cartões é uma fraude onde o criminoso **observa a digitação da senha do cliente** e, durante ou após uma transação, **troca o cartão verdadeiro por um falso** para realizar saques e outras fraudes.



CAPÍTULO 3

Como acontece?

O golpista fica atento enquanto você usa a maquininha de pagamento, observando sua senha.

Após a transação, ele devolve um cartão parecido, mas que não é o seu.

Em caixas eletrônicos, o golpista pode fingir que vai ajudar na operação, enquanto observa a senha digitada.

No final, ele troca seu cartão por outro para usar sua conta indevidamente.

Como se prevenir?

01 Insira sempre você mesmo o cartão na maquininha e mantenha-o sob supervisão o tempo todo.

02 Verifique se o cartão que foi devolvido é realmente o seu antes de se afastar da máquina.

03 Fique atento a pessoas observando você ou olhares curiosos enquanto digita sua senha.

04 Nunca aceite ajuda de estranhos ao usar caixas eletrônicos. Se precisar, peça auxílio a um funcionário do banco devidamente identificado ou a alguém de confiança.

CAPÍTULO 3

3.15 Golpe da Prova de Vida

O que é?

Esse golpe consiste em uma **ligação fraudulenta** em que o **golpista se passa por um funcionário do INSS** para enganar o cliente, alegando a necessidade de realizar a Prova de Vida online ou digital.

CAPÍTULO 3

Como acontece?

O golpista liga para o cliente, dizendo que ele precisa fazer a Prova de Vida Digital para continuar recebendo os benefícios do INSS.

Durante a ligação, pode tentar obter dados pessoais, números de benefício e até solicitar o envio de fotos dos documentos da vítima.

CAPÍTULO 3

Como se prevenir?

01 O INSS nunca entra em contato por telefone para solicitar a realização da Prova de Vida.

02 Caso receba esse tipo de ligação, desligue imediatamente e não forneça nenhuma informação.

03 Nunca informe seus dados pessoais, números de benefício ou envie fotos dos seus documentos por telefone ou mensagens.

CAPÍTULO 3

3.16 Golpe do Cartão Preso no Caixa Eletrônico

O que é?

Nesse golpe, os criminosos se aproveitam de situações em que o **cartão do cliente fica preso no caixa eletrônico**, principalmente fora do horário de expediente. Eles fingem ser funcionários do banco para aplicar a fraude e obter os dados do cartão.

Como acontece?

O golpista se identifica como funcionário do banco e aborda o cliente dentro da agência, mas fora do horário de funcionamento.

Ele informa que o cartão ficou travado na máquina e orienta a vítima a ligar para uma falsa central de atendimento.

Durante essa falsa ligação, a vítima é induzida a fornecer informações do cartão, como número, senha ou outros dados pessoais.

Com essas informações, os criminosos realizam saques, compras ou até contratam empréstimos indevidamente.

CAPÍTULO 3

Como se prevenir?

01 Se seu cartão ficar preso no caixa eletrônico, nunca aceite ajuda de estranhos, especialmente fora do horário de expediente bancário.

02 Não forneça dados do seu cartão ou informações pessoais a terceiros.

03 Faça o bloqueio do cartão imediatamente pelo aplicativo do Banco.

04 Solicite a 2ª via do cartão via canal oficial do banco, durante o horário de atendimento da agência.

Espalhe a segurança:

compartilhe este guia!

Este guia foi feito para te proteger,
e também para ajudar quem você conhece.

Compartilhe com seus amigos, familiares e colegas. **Quanto mais pessoas souberem como os golpes acontecem, mais difícil será para os criminosos agirem.**

Segurança se faz em rede.

Envie este guia para quem você se importa!