CARTILHA DE SEGURANÇA CAIXA

Leia, tire suas dúvidas e compartilhe!

ÍNDICE/SUMÁRIO

#SEGURANÇACAIXA

CAIXA

Há alguns cuidados que podemos tomar para utilizarmos a internet com segurança, mantendo a integridade dos dados e evitando dores de cabeça. Nesta cartilha, ensinamos cuidados essenciais para a proteção de senhas, dados bancários e pessoais. Também vamos apresentar os golpes mais comuns, para que você saiba como se proteger.

1. O QUE SÃO GOLPES?

São práticas criminosas que ocorrem fora do ambiente físico e dos sistemas bancários.

O golpista induz a vítima a fornecer algum dado ou fazer alguma ação que lhe cause prejuízo.

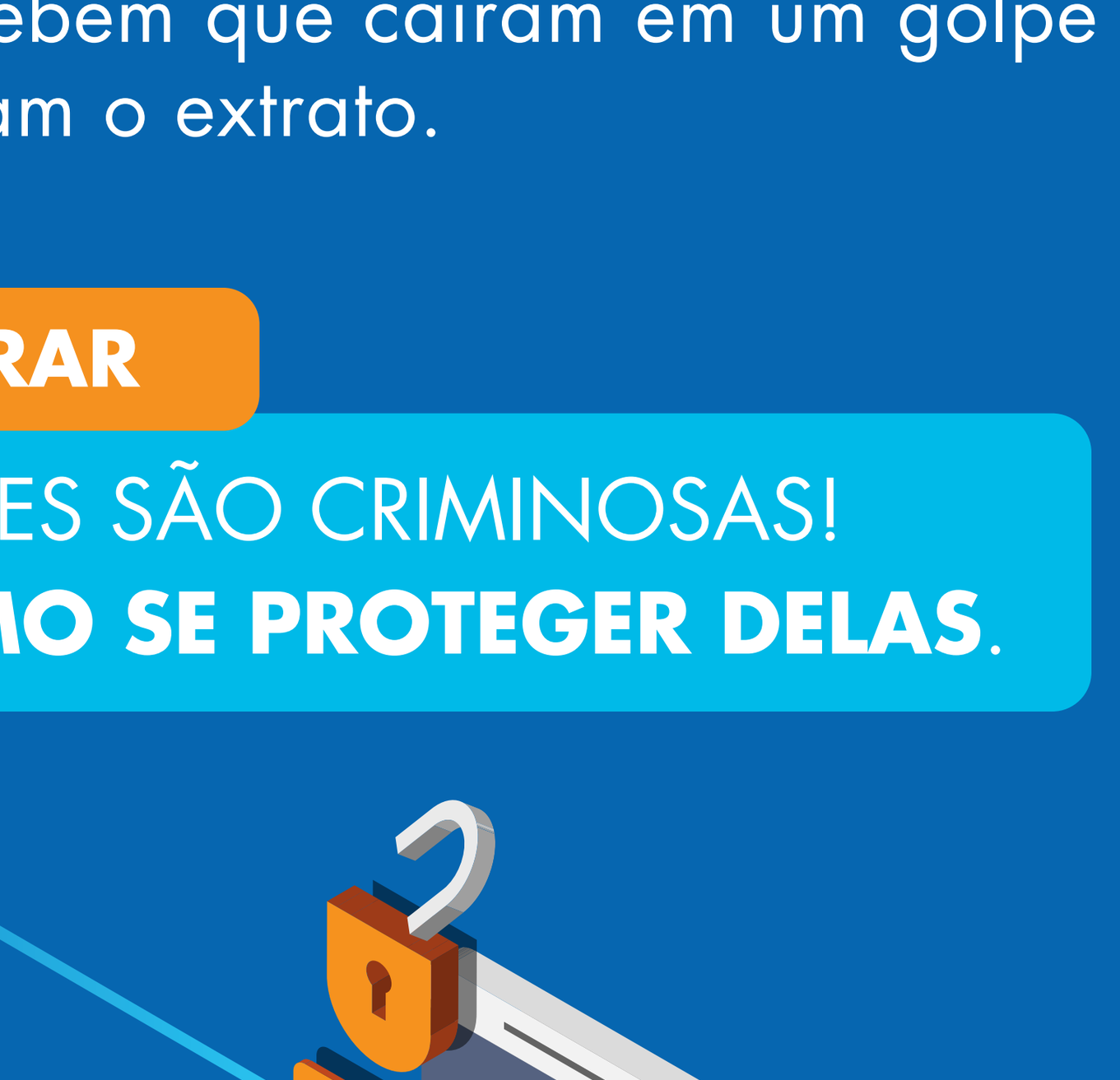
2. COMO OS GOLPES FUNCIONAM

Os golpes podem ser aplicados por mensagens de texto, e-mails, ligações telefônicas e até mesmo presencialmente.

Na tentativa de solucionar o problema, o mais rápido possível, muitas pessoas entregam os cartões, senhas e códigos de acesso às contas bancárias para pessoas desconhecidas, ou que se passam por empregados do banco, e só percebem que caíram em um golpe quando verificam o extrato.

VALE LEMBRAR

ESSAS AÇÕES SÃO CRIMINOSAS!
E TEM COMO SE PROTEGER DELAS.



3. MEIOS **DIGITAIS**

SOU NOVO NO AMBIENTE DIGITAL. **O QUE PRECISO SABER?**

O ambiente digital é repleto de oportunidades e facilidades, mas também tem suas armadilhas. Por isso, para aproveitar todos os recursos digitais disponíveis, é importante se preocupar com a sua segurança.

Alguns sites e redes sociais podem capturar seus dados pessoais, como nome, sobrenome, número de documentos, localização, entre outros, e utilizar essas informações para cometer atos atos ilícitos.

Há alguns cuidados que podemos tomar para navegar com segurança, e evitar dores de cabeça.

Confira nas próximas páginas!

JÁ USO MEIOS DIGITAIS, **TAMBÉM PRECISO ME ATENTAR?**

Até quem já está familiarizado com a internet, aplicativos e sites pode cair em um golpe.

Os golpistas criam páginas e enviam mensagens falsas que parecem verdadeiras. Por isso, as dicas também valem para quem já usa os meios digitais e pode acabar se distraindo e sendo pego de surpresa.

Infelizmente, todos podem ser alvo de um golpe. Dicas de cuidados sempre podem ajudar!

VAMOS CONHECER ALGUMAS DELAS?

4. SENHAS E **AUTENTICAÇÃO**

A senha é uma das formas de verificação da sua identidade, assegurando que você possui o direito de acessar determinado recurso, como sua conta bancária, e-mail, cadastros etc.

A senha pode ser numérica **(apenas números)**, alfanumérica **(letras e números)**, ter caracteres especiais **(@$#ç*%)** ou até mesmo ser configurada por escaneamento facial, escaneamento da impressão digital ou por reconhecimento de voz.

É IMPORTANTE ELABORAR UMA SENHA FORTE, DIFÍCIL DE SER DESCOBERTA E, AO MESMO TEMPO, FÁCIL DE SER LEMBRADA.

LEMBRE-SE

Não tire foto da senha ou de seus dados bancários e não armazene essas informações, nem mesmo em e-mails ou aplicativos de mensagem. Nunca forneça a sua senha para outra pessoa, nem mesmo para atendentes CAIXA.

VEJA O QUE NUNCA UTILIZAR AO ELABORAR SENHAS:

- Qualquer tipo de dado pessoal: evite nomes, sobrenomes, números de documentos, placas de carros, números de telefones e datas;

- Sequências de teclado: evite senhas associadas a botões que sejam próximos, como por exemplo: "**1qaz2wsx**" e "**QwerTAsdfG**", e trechos do alfabeto ou ordem numérica, como "**abcd123**".

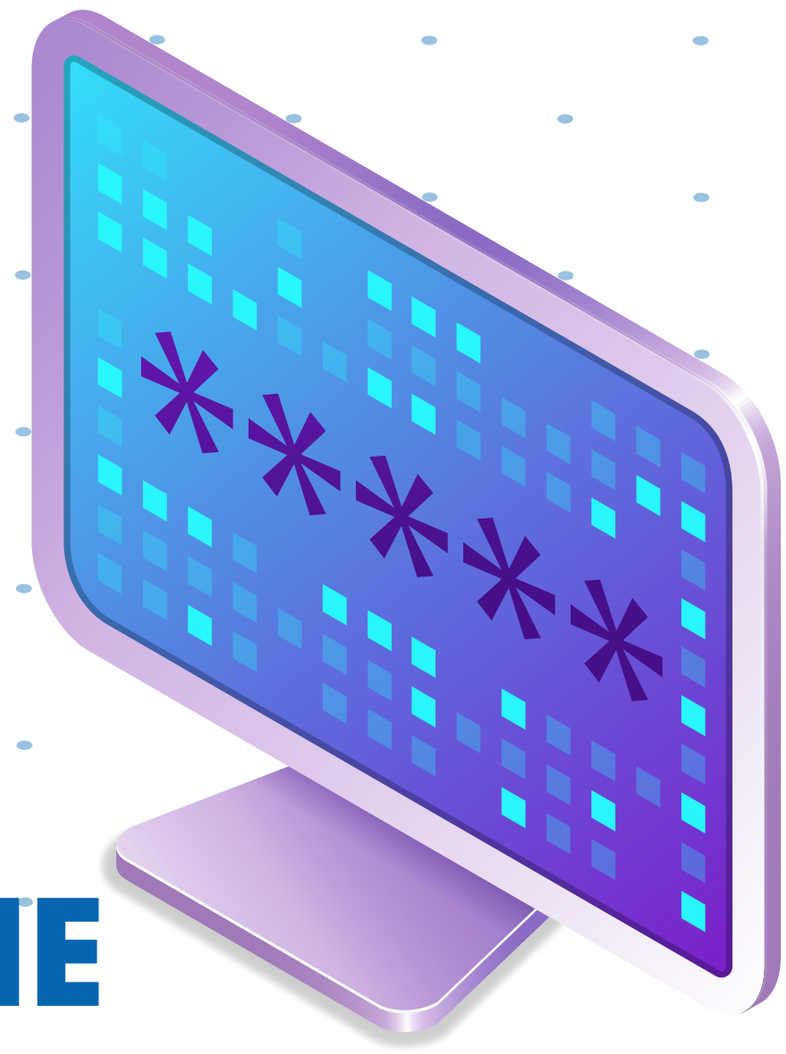
- Termos e nomes publicamente conhecidos: como nomes de músicas, times de futebol, personagens de filmes etc.

AO ELABORAR SENHAS, **SEMPRE USE:**

- Números aleatórios;
- Grande quantidade de caracteres: quanto mais longa for a senha, mais difícil será descobri-la;
- Diferentes tipos de caracteres: procure misturar caracteres como números, sinais de pontuação e letras maiúsculas e minúsculas;
- Troque sua senha periodicamente e não utilize a mesma senha para mais de uma conta ou aplicativo.

#SEGURANÇACAIXA

EM NENHUMA HIPÓTESE UM EMPREGADO CAIXA **PEDIRÁ QUE VOCÊ DIGA OU COMPARTILHE A SUA SENHA.**



Nem no atendimento presencial e nem no atendimento remoto (ex: telefone, e-mail e WhatsApp).

Nunca por aplicativos de mensagens, redes sociais, e-mail ou por outros canais de comunicação.

Se for necessário utilizar a senha em uma transação, ela será sempre digitada pelo próprio cliente no aparelho telefônico, nos aplicativos da CAIXA ou nos momentos de atendimento presencial.

QUANDO A CAIXA LIGA PARA O CLIENTE, **NUNCA PEDE PARA QUE VOCÊ FALE OU DIGITE SUA SENHA NO APARELHO TELEFÔNICO.**

Se isso acontecer, desligue imediatamente. E caso você tenha compartilhado algum dado pessoal ou bancário, como o número do cartão, ligue imediatamente para o SAC CAIXA 0800 726 0101.

#SEGURANÇACAIXA

Se estiver nos terminais de autoatendimento, lotéricas ou Correspondentes **CAIXA Aqui** e tiver dificuldades para realizar transações nos equipamentos, não aceite ajuda de estranhos. Isso vale também para o uso de aplicativos da **CAIXA (CAIXA, CAIXA Tem, Habitação CAIXA, FGTS)**.

Não permita que estranhos tenham acesso ao seu celular. E nunca diga sua senha ou deixe que as pessoas vejam o que você está digitando.

Utilize as regras acima ao usar todos os seus aplicativos, e-mails e perfis em redes sociais. Muitos oferecem a verificação em duas etapas. Ative essa opção sempre que possível.

Evite deixar seus dados e senha salvos para acessos automáticos na próxima vez que você for usar o serviço.

SEGUIR ESSAS RECOMENDAÇÕES PODE GARANTIR **MAIS SEGURANÇA EM SUAS TRANSAÇÕES**

#SEGURANÇACAIXA

5. LINKS **FALSOS**

VOCÊ SABE O QUE É **PHISHING?**

O **Phishing** é o ato ilícito de "pescar" usuários descuidados para roubar informações como: CPF, dados bancários, senhas, números de cartão de crédito e tudo que for necessário para se cometer uma ilegalidade em seu nome.

E, para pescar, é necessário ter uma isca. No caso do Phishing, a isca costuma ser um link **(normalmente uma linha com sublinhado azul que, ao clicar, direciona o usuário para outra página da internet)** enviado por e-mail, mensagens de texto (SMS) ou aplicativos de mensagens. Por isso, fique atento para não clicar em links ou acessar sites suspeitos. Esses links podem redirecionar você para cobranças falsas ou fazer com que você compartilhe informações pessoais e bancárias com um fraudador.

Em caso de tentativa de golpe por Phishing usando o nome da CAIXA, denuncie para **abuse@caixa.gov.br.**

VALE LEMBRAR

A CAIXA nunca envia links por SMS.

PARA EVITAR ESSE TIPO DE GOLPE, FIQUE ATENTO A ALGUMAS INFORMAÇÕES

- Remetentes com endereço de e-mail que imitam a CAIXA. Ex. joaodacaixa@gmail.com, atendimento@caixaeconomica.com e outros. Fique atento! O domínio oficial da CAIXA é @caixa.gov.br

- E-mails de promoções de lojas ou descontos para pagamento em boleto ou Pix com link para acesso direto.

- Mensagens urgentes que falam em clonagem de cartões, compras indevidas, transferências ou cheques de alto valor que trazem links ou telefones de contato. Para entrar em contato com a **CAIXA,** utilize apenas canais e aplicativos oficiais e telefones que estão no site **www.caixa.gov.br** ou no verso do seu cartão.

#SEGURANÇACAIXA

O QUE VOCÊ PRECISA SABER ANTES DE CLICAR EM UM LINK?

- A CAIXA só envia links (por e-mail ou aplicativo de mensagens) se você pedir e autorizar;

- A CAIXA não envia SMS por um número de telefone convencional. SMS CAIXA são enviados SEMPRE por números "diferenciados", por ex.: 29015, 29111, 29193, 29194, 29196 e 29197.

- Recebeu um link por rede social? Confirme se o perfil é mesmo da CAIXA. Todas as páginas da CAIXA são verificadas. Para ter certeza, é só procurar pelo selo azul de verificação ao lado do nome.

Redes sociais oficiais CAIXA

Twitter | Facebook | Instagram | LinkedIn | Youtube

Loterias CAIXA

Facebook | Instagram

CAIXA Investe:

Instagram | YouTube

#SEGURANÇACAIXA

CAIXA

CLIQUEI EM UM LINK DUVIDOSO. E AGORA?

- Encaminhe o e-mail ou tire um print da mensagem recebida, mostrando o número de telefone de onde veio o link, para abuse@caixa.gov.br.

- Feche o site, exclua arquivos e e-mails recebidos. Desinstale aplicativos que tenha baixado por orientação da mensagem duvidosa.

- Passe o antivírus em todos os seus aparelhos digitais (celular, computador, tablet etc.).

A sua segurança é fundamental para a CAIXA!
Se precisar fazer contato com o banco, utilize os canais oficiais CAIXA.

Você encontra todas as formas de atendimento, horários e telefones da CAIXA em www.caixa.gov.br/atendimento.
As equipes da CAIXA estão à disposição e prontas para te atender.

#SEGURANÇACAIXA

CAIXA

6. REDES SOCIAIS **E PRIVACIDADE**

As redes sociais permitem que as pessoas compartilhem fotos, comuniquem-se e se mantenham informadas. Por outro lado, é importante tomar cuidado para que essas informações não sejam utilizadas contra você.

Siga as recomendações do item 4 da cartilha (Senhas e Autenticação) também para suas redes sociais. E atenção:

- Cadastre senhas fortes para seus perfis de redes sociais: use sempre letras e números aleatórios, além de grande quantidade de caracteres, deixando a senha longa. Misture números, sinais de pontuação e letras maiúsculas e minúsculas;
- Habilite a autenticação em duas etapas e não autorize login automático;
- Não compartilhe sua senha com ninguém, nem utilize a mesma senha em várias redes sociais;
- Altere sua senha com frequência e não repita as senhas utilizadas anteriormente;

- Mantenha seus perfis de rede sociais privados, para que somente seus seguidores vejam suas postagens e divulgações;

- Cuidado com aplicativos que solicitam fotos e outras informações pessoais para realizar testes ou avaliações, pois eles podem usar suas informações para fins maliciosos;

- Evite baixar aplicativos em lojas não oficiais.

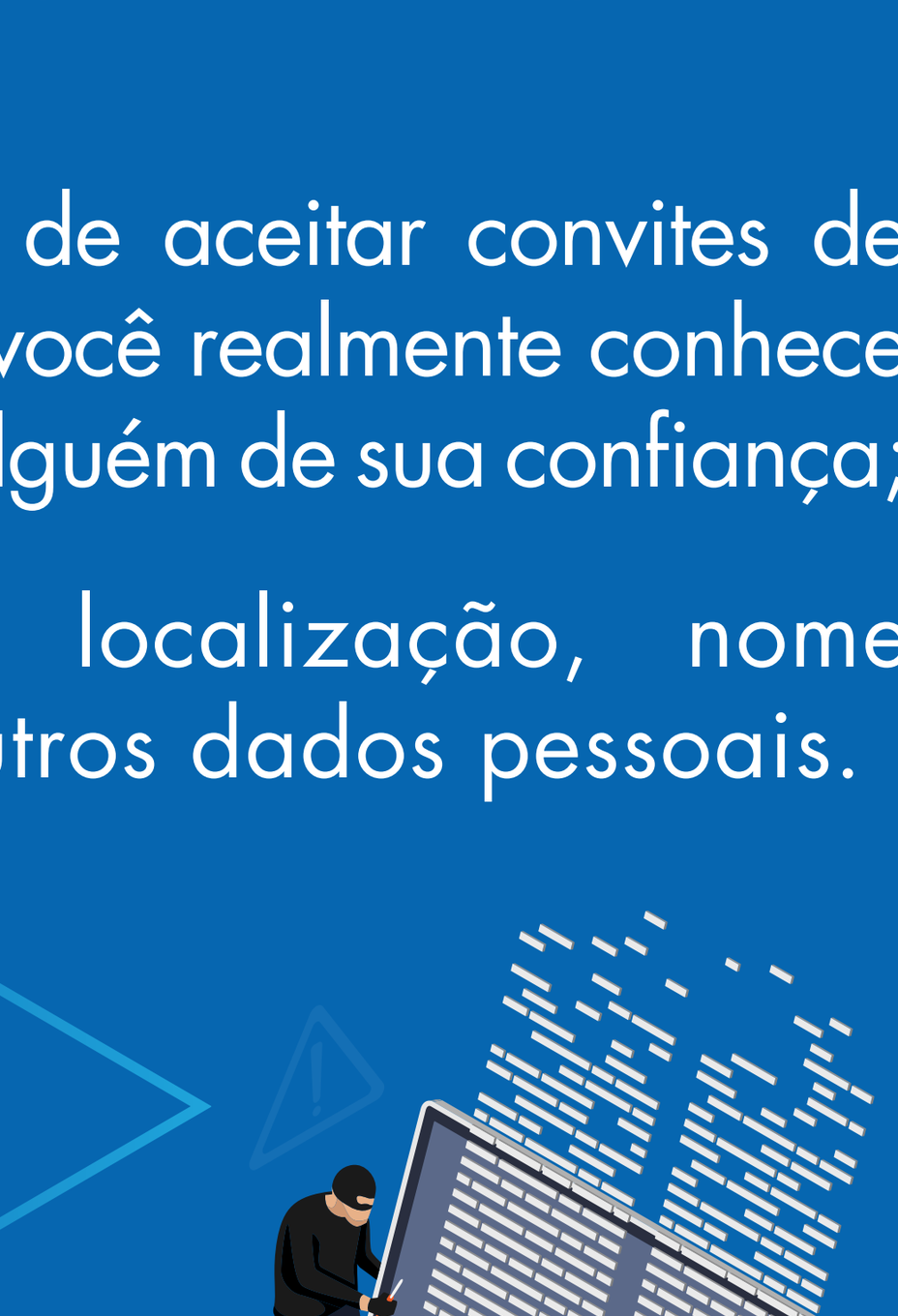
- Evite utilizar redes públicas de internet (Wi-fi gratuito);

- Acesse suas contas apenas em aparelhos pessoais;

- Seja criterioso na hora de aceitar convites de amizade. Só aceite quem você realmente conhece ou quem foi indicado por alguém de sua confiança;

- Evite disponibilizar localização, nome completo, endereço e outros dados pessoais.

Pense sempre que o golpista pode usar essas informações para aplicar golpes usando seus dados e se passando por você.



ESTEJA SEMPRE ALERTA!

#SEGURANÇACAIXA

CAIXA

7. COMO PROTEGER **MEUS DADOS?**

Já ouviu falar em vazamento de dados?

É o que acontece quando informações privadas ou confidenciais são disponibilizadas a uma pessoa não autorizada. O acesso ocorre, geralmente, a partir de uma invasão ao banco de dados onde essas informações estão armazenadas. O vazamento também pode ocorrer quando alguém que tem acesso autorizado, compartilha indevidamente os dados com outra pessoa sem autorização.

O vazamento de dados é um perigo da internet e deve ser uma preocupação para todos os usuários. Se os seus dados forem acessados por criminosos, o seu nome e informações pessoais podem ser utilizados para realizar atos ilícitos.

VEJA ALGUMAS FORMAS DE PROTEGER SEUS DADOS NA INTERNET:

- Ative a autenticação de duas etapas em todos os aplicativos e redes sociais que oferecerem a opção;

- Nunca acesse nem responda mensagens e e-mails de remetentes desconhecidos ou suspeitos;

- Não preencha dados pessoais e bancários antes de ter certeza de que o site ou a loja on-line é confiável. Os golpistas desenvolvem sites e aplicativos muito parecidos com os originais, fique de olho!

- Ao final de qualquer compra on-line, apague do histórico do site e do navegador os seus dados pessoais, números de cartão de crédito ou débito. Evite salvar para compras futuras.

#SEGURANÇACAIXA

8. RECONHEÇA UM **ATENDIMENTO CAIXA**

O QUE A CAIXA PODE FAZER:

- Atendentes CAIXA podem sugerir que você dê prosseguimento a uma solicitação pessoalmente em uma agência ou no aplicativo CAIXA. Eles também podem indicar que você baixe um aplicativo da CAIXA em seu aparelho. Antes de realizar o download*, confirme se está acessando o aplicativo correto.

- Atendentes CAIXA podem solicitar a confirmação de código/token enviado por mensagem, pelos canais oficiais da CAIXA, durante seu atendimento.

Confira aqui todos os **aplicativos oficiais** da CAIXA.

O que é DOWNLOAD: o termo em inglês significa baixar arquivos, transferindo dados de um aparelho para outro.

• Pelos telefones oficiais, atendentes podem solicitar dados pessoais e bancários básicos, como seu nome, informações sobre o seu endereço, a agência da sua conta, se é poupança ou conta corrente, etc. Antes de ligar ou prosseguir com um atendimento por ligação, **veja os telefones oficiais da CAIXA** pelo site CAIXA ou no CAIXA Tem.

O QUE A CAIXA NÃO FAZ?

- Não entra em contato e solicita a sua senha;
- Não recolhe cartões mesmo que estejam cancelados, com defeito, vencidos ou destruídos;
- Não pede aos clientes que façam depósitos em contas bancárias;
- Não envia links por SMS;
- Não envia links para atualização de cadastro, desbloqueio de conta ou cadastramento de chave do Pix;
- Não entra em contato solicitando o desbloqueio de um novo dispositivo para acessar aplicativos ou sistemas do banco, principalmente Internet Banking, aplicativos CAIXA e CAIXA Tem.
- Não solicita o download de nenhum aplicativo que não sejam os oficiais da CAIXA.

#SEGURANÇACAIXA

9. SAIBA COMO **IDENTIFICAR GOLPES** E EVITAR PREJUÍZOS

Além de seguir as orientações desta cartilha, você pode identificar algumas condutas que indicam um possível golpe. **Por exemplo:**

- E-mail com cobrança em que o endereço eletrônico do remetente é longo ou contém números e palavras suspeitas;
- Ligação solicitando senhas;
- Ligações em que alguém envia um link (que não foi solicitado por você) ou informa um código enviado por mensagem sem que haja algum atendimento prévio, pelos canais oficiais da CAIXA;
- Ofertas e empréstimos com condições muito vantajosas;
- Pedidos de dinheiro emprestado por mensagens ou via redes sociais;
- Ligação de um parente distante solicitando ajuda para pagar uma despesa urgente como conta de hospital, de mecânico, etc;
- Se, por telefone, alguém se identificar como empregado CAIXA, solicitando sua senha ou desbloqueio de um dispositivo para acesso à internet;
- Solicitação para que entregue o seu cartão a outras pessoas, mesmo que inutilizados;

- SMS recebido de número não oficial (apresentados na página 13), informando a utilização desconhecida de seu cartão ou conta e solicitando que você entre em contato com um número de telefone não oficial da CAIXA (você encontra os números oficiais no capítulo “RECONHEÇA UM ATENDIMENTO CAIXA”, na página 19.)

- Ligação informando suposto sequestro de familiares ou pessoas conhecidas;

- Pessoas que entram em contato com você e se identificam como alguém conhecido, mas utilizam perfil de rede social, e-mail ou telefone diferentes.

10. O QUE FAZER EM CASO DE **SUSPEITA DE GOLPE?**

- Encaminhe o e-mail ou o print da mensagem recebida do golpista para abuse@caixa.gov.br;
- Bloqueie ou desative o cartão de débito ou cartão de crédito no aplicativo CAIXA ou Cartões CAIXA, respectivamente. Caso não seja possível utilizar os aplicativos, ligue na Central de Atendimento (números disponíveis na página 29) e solicite o bloqueio dos cartões.
- Ligue imediatamente para o SAC CAIXA 0800 726 0101. Informe ao atendente CAIXA tudo o que puder sobre o contato suspeito para que sejam tomadas as devidas providências;
- Faça um Boletim de Ocorrência.

ONDE PROCURAR AJUDA

Em caso de dúvidas sobre segurança, acesse: **www.caixa.gov.br/seguranca**

Caso precise de atendimento, confira os canais digitais, agências e pontos de atendimento mais próximos, telefones, horários de atendimento pre-sencial e remoto e aplicativos da CAIXA em: **caixa.gov.br/atendimento**

#SEGURANÇACAIXA

11. COMO POSSO USAR O MEU CARTÃO **DE FORMA SEGURA?**

CONTROLE A SEGURANÇA DO SEU CARTÃO COM O APLICATIVO CARTÕES CAIXA!

BLOQUEIO TEMPORÁRIO

Está inseguro? Não lembra onde está seu cartão?

É possível bloquear o cartão temporariamente utilizando a opção "BLOQUEIO TEMPORÁRIO", dentro do botão ""Bloquear Cartão" do aplicativo! Dessa forma você impede que o cartão seja usado para novas compras!

Assim que necessário, você pode utilizar a mesma opção para desbloquear o cartão que você bloqueou!

BLOQUEIO DE COMPRAS PELA INTERNET

Quando você quiser impedir que novas compras sejam feitas usando seu cartão na internet, utilize a opção "BLOQUEIO COMPRAS INTERNET", dentro do botão ""Bloquear Cartão" do aplicativo

Assim você pode garantir que o seu cartão esteja liberado para uso na internet apenas nos momentos em que você desejar e se sentir seguro!

COMPRAS POR APROXIMAÇÃO

É possível habilitar ou desabilitar o uso do pagamento por aproximação dos seus cartões utilizando os aplicativos oficiais da CAIXA:

Cartão de Crédito: Utilize o botão "Desativar aproximação" do aplicativo Cartões CAIXA

Cartão de Débito: Utilize a opção "Pagamento por aproximação" do menu "Cartão de Débito" do aplicativo CAIXA (Internet Banking)

ACOMPANHE SUAS COMPRAS

A CAIXA envia SMS com os dados da transação sempre que uma compra com seu cartão de crédito é realizada e, no cartão de débito, sempre que o valor alcançar o limite que você definir na opção "Mensagens via celular", do aplicativo CAIXA!

Você também pode acompanhar as suas compras por meio dos cartões nos nossos aplicativos oficiais!

- Cartão de Crédito: Suas compras são exibidas na tela inicial do aplicativo! Se você possuir mais de um cartão, é só deslizar para o cartão desejado na tela principal para visualizar as compras realizadas com ele.

- Cartão de Débito: Utilize tanto a opção "Extrato", na tela inicial, quanto a opção "Últimas Compras" do menu "Cartão de Débito" do aplicativo CAIXA (Internet Banking)

CONTROLE A SEGURANÇA DO SEU CARTÃO COM O APLICATIVO CARTÕES CAIXA!

COMPRAS SEGURAS NA INTERNET

Seu cartão tem três chaves para que uma compra na internet seja feita:

- Número completo do cartão
- Data de Validade
- Código de segurança

Seja cauteloso em informar esses dados, evitando tanto o compartilhamento com outras pessoas, quanto informar em sites duvidosos.

Dê preferência aos sites de lojistas conhecidos e avalie cuidadosamente sites em que estiver fazendo compra pela primeira vez. Ofertas tentadoras e grandes descontos podem indicar uma situação suspeita, Desconfie!

Ao comprar em lojas online opte pelo uso do cartão virtual do aplicativo Cartões CAIXA, assim você protege o seu cartão físico, evitando sua exposição a riscos de fraude!

Lembre-se, a qualquer sinal de insegurança, você pode bloquear seus cartões nos aplicativos da CAIXA!

#SEGURANÇACAIXA

Para atendimentos relacionados aos **Cartões CAIXA**, contate os números de telefone abaixo:

Cartão
Azul
Nacional
CAIXA Sim
Internacional
Gold
Elo Mais

Cartão
Platinum
Elo Grafite
Mastercard Black
Visa Infinite
Elo Nanquim
Elo Diners Club

Cartão
Elo Empresarial
Elo Empresarial Mais
Elo Empresarial Grafite:

4004 0 104
(capitais e regiões metropolitanas)

0800 104 0 104
(Demais regiões. O atendimento ocorre 24 horas por dia, 7 dias por semana)

0700 726 2492
Atendimento a clientes portadores de deficiente auditiva e/ou de fala

55 61 2106 0999
Atendimento Cartões CAIXA no Exterior (ligação a cobrar)
*A ligação pode ser feita a cobrar. Consulte a forma de ligação a cobrar do país de onde fará a chamada.

APLICATIVOS DA CAIXA

#SEGURANÇACAIXA

WhatsApp CAIXA: 0800 104 0 104

Converse com a CAIXA pelo WhatsApp no número **0800 104 0 104**.

Salve esse número no seu celular e observe que nosso número é verificado.

A CAIXA só poderá entrar em contato com você por este canal, após a sua autorização.

Confira o nome do contato "Atendimento CAIXA" e o símbolo verde "✔", que indica que é uma conta comercial oficial no WhatsApp.

Fique atento, no atendimento realizado através do WhatsApp CAIXA, em nenhum momento, será solicitada a sua senha bancária ou a senha de seu cartão.

#SEGURANÇACAIXA

12. CONHEÇA OS GOLPES MAIS COMUNS

Link Falso

Golpistas podem enviar links falsos por e-mail, por redes sociais, WhatsApp ou SMS. Esses links normalmente solicitam atualização de dados, pagamento ou apresentam promoções tentadoras e podem conter vírus ou outras ameaças que roubam informações pessoais dos usuários.

Nunca clique em links enviados por desconhecidos!

Se suspeitar de golpe, encaminhe o e-mail ou tire um print da mensagem recebida, mostrando o número do telefone de onde veio o link falso, e faça uma denúncia para **abuse@caixa.gov.br.**

Compra Falsa

Golpistas entram em contato fingindo ser um empregado ou gerente do banco e avisam sobre uma suposta compra realizada com o cartão do cliente. Na conversa, além de confirmar dados pessoais, o criminoso pede informações como número do cartão e **CVV*.** Com esses dados, o golpista pode realizar compras na internet.

Nunca informe seus dados pessoais ou bancários para número de telefone divergente dos telefones oficiais da CAIXA!

Para acompanhar as movimentações da sua conta, baixe os aplicativos CAIXA e Cartões CAIXA, vá à agência mais próxima ou entre em contato com a Central de Cartões.

***O que é CVV**: esta é a sigla para "Card Verification Value", conhecido como "código de verificação" em português. São três números presentes na parte de trás do cartão, que funcionam como proteção para compras on-line. Por isso, nunca compartilhe esse dado com ninguém!

Doação Irregular

Se passando por integrantes de ONGs, fundações, creches e abrigos, golpistas ligam pedindo apoio e doações para a instituição. Os criminosos informam um número de conta para que a vítima realize o depósito.

Para se proteger desse tipo de golpe, **nunca realize depósitos ou transferências para contas desconhecidas!**

Falsas Centrais

Para obter informações sensíveis, como número de contas, CPF e senhas ou mesmo, acesso remoto aos dispositivos e contas, golpistas conseguem mascarar o número real do telefone que está originando a ligação, simulando que o contato seja de uma das Centrais de Atendimento da CAIXA e entram em contato se passando por empregados do banco.

Golpistas também podem enviar mensagens por SMS informando que transações via Pix ou operações com o cartão estão em análise e que para cancelar é necessário ligar na central de atendimento, cujo número não corresponde aos números oficiais da CAIXA.

Atenção: a CAIXA só envia mensagens SMS pelos pelos números: 29015, 29111, 29193, 29194, 29196 e 29197. Os telefones oficiais da CAIXA estão impressos no verso do seu cartão, bem como no SITE **www.caixa.gov.br/atendimento**.

A CAIXA não solicita acesso ao dispositivo, nem solicita desbloqueio de um novo dispositivo para acessar aplicativos ou sistemas do banco.

A CAIXA não faz ligação para os clientes a partir de números das Centrais de Atendimento. Caso receba uma ligação com a identificação que foi originada por uma Central da CAIXA, desligue e imediatamente ligue para o SAC CAIXA 0800 726 0101.

As Centrais de Segurança dos Cartões CAIXA, podem entrar em contato com você para confirmar transações ou alterações cadastrais realizadas no cartão de crédito, mas atenção: empregados CAIXA **nunca pedem senha ou o número completo do cartão.** Nunca compartilhe sua senha e dados bancários por telefone!

Golpe da Troca de Cartão

Golpistas oferecem ajuda para as vítimas no autoatendimento. O criminoso, geralmente bem vestido ou com crachá e uniforme falsos, pede o cartão da vítima e o troca por outro. Depois da troca, deixa o local e utiliza o cartão roubado para sacar ou transferir os valores da conta.

Principalmente em uma agência fechada, não aceite ajuda de ninguém! **Quando precisar de atendimento, busque sempre empregados da CAIXA.**

Golpe da Tela Aberta

Também no autoatendimento, o golpista oferece ajuda se passando por empregado do banco. Com o cartão do cliente já inserido no terminal, realiza transferências de valores para outras contas, sem que a vítima perceba.

Nunca aceite ajuda de estranhos, mesmo dentro das agências. Ao utilizar o terminal de autoatendimento não se esqueça de finalizar o atendimento antes de sair do terminal e verifique se o cartão é realmente o seu.

Golpe do Cartão Preso na Máquina

Criminosos instalam aparelhos no terminal de autoatendimento, com o objetivo de reter o cartão do cliente na leitora, orientando-o a ligar para uma central falsa para resolver um problema. Com a ligação, o golpista obtém os dados necessários do cliente.

Caso o cartão fique preso na máquina, informe um funcionário da agência.
Se a agência estiver fechada, entre em contato com a central de atendimento CAIXA (confira no item 10).

Golpe do telefone celular clonado

Chamado de **SIM Swap**, esse golpe consiste na clonagem do número de um celular. Com um chip em branco e dados do usuário, o golpista liga para a operadora telefônica e se passa pela vítima, solicitando a ativação do número no novo chip. Assim, o golpista tem acesso a ligações, mensagens e tokens (confira o item 8 da cartilha).

Se seu celular ficar fora de conexão ou sem sinal por muito tempo, entre em contato com a operadora para verificar se foram habilitados novos cartões SIM sem sua autorização. E fique atento também às transações realizadas no seu cartão de crédito durante este período. Você pode consultar sua fatura no IBC ou aplicativo Cartões Caixa.

O que é TOKEN:

código numérico enviado **via SMS** com objetivo de validar a ativação de uma conta ou serviço em atendimentos remotos.

Fraude do Extravio de Cartões

O criminoso intercepta a correspondência de entrega do cartão e liga para o cliente se passando por empregado CAIXA, informando dados verdadeiros, e afirma que, para receber o novo cartão, a vítima precisa digitar alguns dados no telefone. Com esses dados, os golpistas podem realizar compras, saques e transferências.

Se receber uma ligação suspeita, contate a Central de Atendimento CAIXA.

Lembre-se: a CAIXA nunca solicita que o cliente digite a senha do cartão no telefone ou a informe por ligação.

Golpe do Consórcio ou Carta Premiada

A partir de propagandas em redes sociais, jornais, aplicativos de vendas e outros meios, golpistas oferecem cartas contempladas e prometem liberação de crédito para compra de algum bem (veículo, por exemplo) mediante o pagamento de um valor como entrada. A vítima acredita se tratar de uma transação verdadeira, e após assinar um suposto contrato de compra e pagar a entrada, descobre que foi enganada, pois o golpista some com o valor.

Antes de fechar qualquer negócio envolvendo consórcio, confira no site do Banco Central se a instituição existe e se está autorizada a fazer esse tipo de operação. Procure saber se a administradora do consórcio é associada à ABAC (Associação Brasileira das Administradoras de Consórcio).

Falsa Venda

Copiando um anúncio verdadeiro, o golpista se passa por vendedor com preços bem abaixo do mercado. Ao ser contatado por pessoas interessadas, o golpista negocia os valores; o comprador realiza o pagamento conforme solicitado e, após receber, o golpista apaga o anúncio. Ao procurar o vendedor, a vítima encontrará apenas o anunciante verdadeiro, que normalmente não tem relação com o golpista.

Realize compras apenas em sites confiáveis e que dão garantias à compra e venda de produtos. **Desconfie de promoções e de valores muito vantajosos.**

Site Falso

Golpistas criam sites idênticos aos reais para enganar a vítima. No link do site, alteram apenas alguns detalhes para que a farsa passe despercebida. Esse tipo de ação acontece todo ano, mas é intensificada durante as campanhas da semana do consumidor e da Black Friday, quando as compras on-line aumentam.

Antes de colocar seus dados e clicar em links, ou realizar compras, **verifique o endereço eletrônico do site!**

Falso Empréstimo

Promessas de liberações de crédito ou antecipações de empréstimo mediante depósito antecipado, principalmente para pessoas negativadas, podem ser golpes!

Os golpistas solicitam os dados pessoais, bancários e fotografias das vítimas, sendo comum enviarem um formulário através de link do WhatsApp e abrem contas nos nomes das vítimas. A partir daí, faz contratação de empréstimo, sem a permissão da vítima, que quase sempre é orientada a depositar valores em uma conta bancária, sem nenhuma garantia.

Fique atento aos empréstimos com condições duvidosas ou orientações suspeitas de depósitos de valores em conta bancária!

Falsas Premiações e Sorteios

Mensagens que informam que você foi sorteado e trazem a frase "você ganhou!" podem ser golpes em busca de dados pessoais e bancários.
As Loterias CAIXA, por exemplo, nunca enviam mensagens sobre resultados de sorteios e não divulgam nomes de premiados em sorteios para garantir a segurança do usuário de produtos de loterias.

Desconfie de premiações e sorteios de empresas desconhecidas! Sempre confira a procedência.

#SEGURANÇACAIXA

Golpe do Código por SMS ou Aplicativos de Mensagens

Se receber códigos de acesso às suas contas, por SMS ou aplicativos de mensagens, não compartilhe com outras pessoas. Golpistas podem utilizar esses códigos para acessar suas contas de redes sociais e aplicativos de bancos.

Esse código é pessoal, exclusivo, costuma ter 6 dígitos e serve para ativar/acessar sua conta no nos aplicativos

Golpe do Motoboy

O golpista liga se passando por um funcionário do banco ou da administradora de cartões, muitas vezes informando os dados verdadeiros do cliente e afirma que o cartão foi clonado ou que há compras suspeitas, sendo necessário o cancelamento do cartão. Para efetuar o cancelamento, solicita ao cliente que digite alguns dados no telefone, entre eles a senha do cartão, e para concluir o cancelamento, orienta o cliente a cortar o cartão ao meio que um motoboy irá buscá-lo na residência do cliente ou em outro local para segurança da operação. Com os dados do cliente, a senha e o chip em mãos, o criminoso faz diversas compras no cartão.

Nunca entregue seu Cartão inutilizado para outras pessoas.

Ao descartar seu cartão, corte o chip no meio.

Dinheiro Emprestado

Golpistas podem clonar os aplicativos de mensagens de pessoas e se passarem por elas, fingindo dificuldades financeiras. Nesse tipo de golpe, o criminoso pede dinheiro emprestado aos contatos cadastrados no celular da vítima.

Se receber uma mensagem desse tipo, ligue para a pessoa e confirme se é realmente ela quem está mandando a mensagem. **Desconfie de pedidos urgentes por dinheiro.**

Golpe do Bilhete Premiado

Golpistas podem abordar pessoas na rua informando possuir um falso bilhete de loteria premiado e que, por algum motivo, não podem recebê-lo na agência bancária. Os criminosos prometem a divisão do falso prêmio com a vítima desde que ela dê um determinado valor em dinheiro como garantia. Após a vítima ser convencida a entregar o valor da garantia, os criminosos desaparecem.

Não dê dinheiro a qualquer pessoa por supostos bilhetes premiados.

Golpe do Falso Boleto

Golpistas podem enviar, por e-mail ou até mesmo pelos correios, um boleto de cobrança falso.

Antes de pagar, verifique se a dívida é devida e, antes de confirmar o pagamento do boleto, confira se o banco que aparece na tela de pagamento é o mesmo que está no documento. **Confira o valor, a data de vencimento, o nome do beneficiário e demais dados.**

Golpe do falso brinde

Os golpistas se passam por funcionários de grandes lojas, parabenizando o aniversariante e oferecendo um presente ou brinde em comemoração, que será entregue por um motoboy.

Para receber o brinde, o golpista vai solicitar "apenas" o pagamento da taxa de entrega, que só pode ser feito por cartão de crédito.

No momento da entrega, o golpista vai utilizar o golpe da maquininha para tentar enganar a vítima e realizar diversas transações no cartão.

Golpe da Maquininha

O golpista se utiliza de uma "maquininha de cartão," com o vidro do visor danificado e/ou com obstruções (tinta, adesivos, etc.), e se aproveita da dificuldade de visão do cliente, ou de uma distração, e digita um valor maior para o pagamento da transação;

Este tipo de golpe, costuma ser praticado em serviços de entregas. Dê preferência para pagamentos online, direto pelo aplicativo do estabelecimento, bem como desconfie de cobranças adicionais, como taxas extras ou pedidos de gratificações ("caixinhas");

- Ative o SMS, para receber as notificações de pagamentos realizadas com seu cartão.

Golpe do Falso Presente

Os golpistas se passam por entregadores, para receber o presente inesperado o entregador informar que precisa tirar uma foto da pessoa com o presente para comprovar a entrega.

Com essa foto em mãos, o golpista pode abrir contas e fazer empréstimos em bancos digitais em nome da vítima.

BOLETOS

A CAIXA só envia boletos criptografados, seja a fatura de seu cartão ou a renegociação de uma dívida; para acessá-los, basta digitar o seu CPF.

Os boletos CAIXA têm características específicas que evitam adulterações e permitem a você diferenciar o original e escapar de possíveis golpes.

Para saber se o boleto é mesmo da CAIXA, confira a marca do banco no documento, o código do banco (104-0) e a representação numérica do boleto (que sempre começará com 104).

Antes de pagar, verifique também se a dívida é devida e, antes de confirmar o pagamento do boleto, confira os dados do beneficiário (nome ou razão social e CPF/CNPJ), valor e data de vencimento."

A marca da CAIXA é sempre esta

O Código da CAIXA é sempre 104-0

Os três primeiros números da linha digitável são 104

13. O QUE A CAIXA FAZ PARA **GARANTIR SUA SEGURANÇA**

NAS AGÊNCIAS

As **agências CAIXA** possuem equipamentos de segurança e equipe de vigilância treinada para identificar situações de risco potencial contra empregados e patrimônio, notificando as Centrais de Monitoramento quando necessário para atuação junto aos órgãos de segurança pública.

CHEQUE

Assim como os boletos, os cheques CAIXA também possuem itens de segurança exclusivos, que dificultam reproduções não autorizadas. Atente-se às cores, tipo de papel, marca d'água. O padrão é o seguinte:

- A frente e o verso das folhas de cheque possuem cores diferentes, que evidenciam qualquer traço de apagamento por lavagens químicas ou rasura;

- As folhas de cheque são feitas em papel-moeda (o mesmo das cédulas do real);

- No interior da folha de cheque, o padrão da filigrana contém a marca d'água, constituída por figuras da logomarca "CAIXA", e as três linhas, denominadas "linhas loucas", apresentando cruzamento entre si, que podem ser visualizadas quando exposta à claridade;

- Na frente da folha de cheque, o padrão tem duas "linhas loucas" impressas, localizadas no lado direito do formulário, contínuas, variáveis e sinuosas, que nunca se cruzam.

SMS (Mensagens de texto)

A **CAIXA** possui serviço de mensagens via celular para garantir mais praticidade e segurança para as transações. Ao se cadastrar, você recebe mensagens de alerta sobre todas as transações efetuadas com os cartões de débito ou crédito, compras aprovadas, canceladas, negadas e transações via Pix.

Atenção: a CAIXA só envia mensagens pelos números: **29015, 29111, 29193, 29194, 29196 e 29197**. Se receber conteúdos de outros contatos por SMS, denuncie (veja como no item 10 da cartilha) e não clique em links nem confie nas informações recebidas.

Para cadastrar o serviço de mensagens, utilize seu cartão no terminal de autoatendimento e escolha a opção "**Outros Serviços**" > "Mensagens via celular". Cadastre seu número de celular e selecione o valor mínimo para recebimento de SMS para transações.

Se a CAIXA enviar um SMS sobre alguma movimentação financeira ou compra que você não fez, **responda ao SMS recebido,** conforme orientações, solicitando o bloqueio da sua senha e/ou cartão.

Na dúvida ligue para os números da CAIXA disponíveis em nossos canais oficiais.

14. E O PIX É SEGURO?

O Pix conta com diversos mecanismos de segurança, sendo que vários foram desenvolvidos exclusivamente para ele:

- A identidade do pagador é autenticada digitalmente, por senha, antes de qualquer pagamento ou transferência.

- Os dados das transações do Pix transitam criptografados na Rede do Sistema Financeiro Nacional, que é uma rede segura de dados operada pelo Banco Central.

- O Pix conta com "motores antifraude" que permitem identificar transações fora do perfil do usuário, bloqueando para análise as transações suspeitas por até 30 minutos durante o dia, ou 60 minutos à noite e rejeitando aquelas que não se confirmarem uma transação segura.

#SEGURANÇACAIXA

- O Pix possui, em sua base de dados, mecanismos de proteção que impedem o roubo de informações pessoais dos clientes.

- Em caso de confirmação de fraude a chave Pix utilizada na transação é marcada e informada para todas as instituições financeiras participantes do sistema.

- As transações são rastreáveis, o que permite a identificação do recebedor dos recursos originados de fraude/golpe/crime e a ação mais incisiva da polícia e da Justiça.

- E há limites máximos de valor para transferências, pagamentos ou saque via Pix, com base no perfil de cada cliente, no período do dia em que ocorre a transação, canal de atendimento ou a forma de autenticação do usuário.

Mas fique ligado:

Confira sempre o nome do destinatário e não transfira valores para desconhecidos.

A CAIXA não envia links para você atualizar cadastro ou criar chaves Pix.

No momento do cadastramento, você receberá um código Token para validação da posse da chave Pix por mensagem de e-mail ou celular. Esse token não deve ser compartilhado.

#SEGURANÇACAIXA

CAIXA