Sicredi | Pioneira desde 1902

Cartilha de segurança digital

Dicas práticas para ajudar no **combate às fraudes e golpes**

Juntos pela sua proteção no ambiente digital.

Em um mundo cada vez mais conectado e digital, proteger-se é essencial.

Estar bem informado sobre as principais práticas de segurança digital e atento aos golpes mais comuns é o primeiro passo para garantir a proteção dos seus dados bancários e pessoais. A proteção dos seus dados, assim como dos nossos associados, é fundamental.

Pensando nisso, para garantir o cuidado que essas informações merecem, essa cartilha traz **dicas para evitar fraudes e golpes em ambientes digitais**, aumentando a sua segurança e a dos nossos associados em suas transações.

Boa leitura!

Sicredi | Pioneira desde 1902

Cartilha de **Segurança Digital**

mandamentos da segurança digital

Não compartilhe suas senhas, tokens ou códigos de autenticação com ninguém.

Verifique a segurança do site. O "s" do "https" é um indicativo de que o endereço é seguro.

Crie senhas fortes e difíceis de adivinhar. Evite usar a mesma em mais de um lugar.

Nunca clique em links desconhecidos recebidos por e-mail, WhatsApp ou redes sociais.

Use autenticação em dois fatores em todas as contas importantes.

Atualize seus aplicativos, navegadores, sistemas operacionais e antivírus **com frequência**.

Evite usar Wi-Fi público para transações bancárias. Prefira redes seguras e privadas.

Cheque os dados do recebedor antes de finalizar um PIX ou pagamento.

Baixe aplicativos apenas das **lojas oficiais**.

Desconfie de pedidos de dinheiro por mensagem. Sempre ligue e confirme com quem pediu.

Em caso de dúvida, entre em contato com a gente pelos canais oficiais do Sicredi.

Cuidar da sua **segurança** é **nosso compromisso!**

Como nós protegemos nossos associados:

Alerta ao enviar Pix
Ao iniciar o pagamento via Pix, caso seja informada uma chave denunciada por outra instituição, será emitido um alerta na tela.

Aplicativo bloqueado em ligação
O aplicativo Sicredi é capaz de identificar quando um telefone está em ligação ativa e o associado tenta realizar login no app.

Origem Verificada
Esse sistema autentica informações do telefone de origem, exibindo dados confiáveis no identificador de chamadas do destinatário.

Cartão virtual
para compras online com mais segurança.

Notificações em tempo real
de movimentações financeiras.

Educação sobre segurança digital por meio de blogs, redes sociais e materiais informativos.

Sicredi | Pioneira desde 1902

Dicas práticas

para ajudar no combate às **fraudes e golpes:**

Ative a chave Pix **somente nos nossos canais oficiais** e não realize nenhuma transação de teste. Sempre **confirme os dados do recebedor**.

Habilite a **verificação em duas etapas** no WhatsApp.

iOS (quando você tem um Iphone): no WhatsApp, acesse Ajustes > Conta > Confirmação em duas etapas > Ativar.

Android (quando você tem outro modelo de celular): no WhatsApp, acesse Menu > Configurações > Conta > Confirmação em duas etapas > Ativar.

E, para evitar que sua **foto no WhatsApp** seja utilizada indevidamente, **exiba somente para seus contatos de confiança.**

iOS (quando você tem um Iphone): no WhatsApp, acesse Ajustes > Conta > Privacidade > Foto de Perfil > Meus contatos.

Android (quando você tem outro modelo de celular): no WhatsApp, acesse Menu > Configurações > Conta > Privacidade > Foto de Perfil > Meus contatos.

Se receber alguma solicitação para realizar transações, **confirme a legitimidade do pedido da transferência ou pagamento ligando para a pessoa e fazendo perguntas pessoais**. Mesmo que a foto do contato seja da pessoa que você conhece, faça a confirmação antes de realizar a transação.

Ao realizar um pagamento de boleto, **certifique se a linha digitável está de acordo com o logo da instituição financeira**, além do Beneficiário - Cedente e Pagador – Sacado.

Sicredi | Pioneira desde 1902

Atenção aos sites que possuem domínio **.com** e produtos com valores muito abaixo do praticado.

Ao acessar sites, **procure sempre digitar o endereço no navegador.** Evite clicar em links.

Proteja seu computador, não abra arquivos de fontes desconhecidas.

Nunca forneça senha ou dados pessoais a terceiros, principalmente por telefone.

Desconsidere mensagens de instituições financeiras com os quais você não tem relação, especialmente quando solicitarem seus dados pessoais ou a instalação de módulos de segurança.

Não faça transações bancárias a partir de equipamentos de terceiros ou redes Wi-Fi públicas.

Nunca entregue seu cartão a outra pessoa. Nenhuma instituição financeira faz coleta de cartões.

Sempre corte o chip do cartão ao descartá-lo.

Ao utilizar o recurso de login por biometria, **esteja ciente que toda biometria cadastrada em seu celular terá acesso aos aplicativos** em que você utiliza essa funcionalidade. Em caso de perda ou roubo do celular, comunique imediatamente sua instituição financeira para solicitar o bloqueio da conta e acesso ao aplicativo, evitando assim a utilização indevida por terceiros.

Ao fazer uma negociação, confirme o efetivo recebimento do dinheiro em sua conta antes de entregar a mercadoria. Tenha atenção a comprovantes falsos, comprovantes de agendamento ou comprovante de depósito feitos em caixa eletrônico utilizando um envelope vazio.

Trocar senhas periodicamente (a cada 2 meses, ou sempre que houver suspeita de que sua senha foi comprometida).

Sicredi | Pioneira desde 1902

Não compartilhe senhas e nem utilize a mesma senha para vários serviços.

Não salve senhas em cadernos, arquivos, no celular ou navegador.

Crie senhas difíceis de serem descobertas. Utilize letras (maiúsculas e/ou minúsculas), números e caracteres especiais quando for permitido.

Utilize Gerenciadores de senhas, pois eles criptografam credenciais e geram senhas complexas e aleatórias.

Em caso de perda ou roubo do celular, **comunique imediatamente sua instituição financeira para solicitar o bloqueio da conta e acesso ao aplicativo,** evitando assim a utilização indevida por terceiros.

Você é responsável pela movimentação financeira da sua conta. Não empreste a terceiros para receber valores que você desconheça a origem e não saiba a procedência.

Cartilha de **Segurança Digital**

Golpe ou fraude

Qual é a diferença entre golpe e fraude?

GOLPE

- O criminoso tem algum contato com a vítima para praticar o golpe.
- Usa a pessoa em questão para obter informações, senhas e outros dados justamente para fazer transações que tiram dinheiro da vítima.
- **Exemplos:** WhatsApp, leilão, sites de venda, motoboy, falso empréstimo, falso sequestro, bilhete.

FRAUDE

- O criminoso realiza transações sem ter acessado propriamente a vítima.
- O fraudador tem posse dos dados para obter ganhos financeiros sem precisar ter tido contato algum.
- **Exemplos:** Engenharia social com falsa central, clonagem de cartão, pirâmide financeira, roubo de dados via ligações e sites falsos, boletos falsos.

Sicredi | Pioneira desde 1902

Cartilha de **Segurança Digital**

Fique por dentro dos golpes mais comuns e saiba como se proteger!

- Golpes com Cartões
- Golpes com Falsos Funcionários
- Golpes por WhatsApp
- Golpes de Phishing
- Golpes de Sites Falsos
- Golpes do Boleto Falso
- Engenharia Social

Sicredi | Pioneira desde 1902

Golpes com Cartões

Como acontecem:

Você sabia que os golpes com cartões podem acontecer em situações comuns, como em lojas, no caixa eletrônico ou até mesmo durante a entrega do cartão? Por isso, **é essencial ficar atento.**

Falso motoboy:

Se receber uma ligação dizendo que há transações suspeitas em seu cartão e que será enviado um motoboy para coletá-lo, **não passe informações (especialmente sua senha) e desligue na hora**. Lembre-se de que **nenhuma instituição financeira tem essa prática**.

No comércio:

O golpista observa sua senha e, na hora de devolver o cartão, entrega um muito parecido mas, que não é o seu. Às vezes, também usam de alguma distração para pedir que você digite a senha no campo de valor.

No caixa eletrônico:

Algumas pessoas mal-intencionadas se oferecem para "ajudar", mas o real objetivo é ver sua senha e trocar seu cartão.

Compras on-line:

Se o golpista conseguir seus dados do cartão (nome, número, validade e código de segurança), pode usá-los para fazer compras pela internet.

Na entrega do cartão:

Em certos casos, golpistas interceptam cartões antes de chegarem às mãos dos verdadeiros donos. Depois, entram em contato fingindo ser do banco, pedem para desbloquear o cartão e passam a usá-lo indevidamente.

Voltar ao menu

Como se proteger!

Cuidado com o golpe do motoboy. **Nós não realizamos a retirada do seu cartão**. **Nunca entregue seu cartão** para ninguém. Caso precise descartá-lo, **corte o chip antes**.

Preste muita atenção na hora de fazer qualquer compra, seja ela física ou on-line.

Verifique se está digitando a senha no campo correto e confira o seu cartão na devolução.

Jamais desbloqueie um cartão que não esteja em suas mãos.

Nos terminais de atendimento, não aceite a ajuda de estranhos. **Se precisar de auxílio, sempre recorra a um funcionário identificado**.

Nunca divulgue os dados do seu cartão para outras pessoas ou em redes sociais.

Utilize um cartão virtual para suas compras on-line. Com ele, você tem mais praticidade e maior segurança, e suas compras com cartão virtual vêm na mesma fatura do seu cartão físico.

Golpes com Falsos Funcionários

Como acontecem:

Golpistas se **passam por funcionários da instituição financeira** para obter informações confidenciais. Podem dizer que trabalham na área de segurança e que precisam confirmar supostas transações realizadas. **A intenção dos golpistas é coletar informações pessoais e dados bancários para utilização indevida.**

Como se proteger!

Nunca forneça informações por telefone, ou através de links recebidos por SMS, WhatsApp, e-mails, redes sociais, entre outros. Não digite seus dados em uma suposta central de atendimento.

Nesse tipo de golpe, **os golpistas podem até simular o número de telefone** da instituição financeira e usar recursos tecnológicos, como gravações e menus para aumentar a sua confiança.

Lembre-se!

Nós entramos em contato com você, mas nunca para realizar:

- **Atualização do módulo de segurança;**
- **Atualização cadastral;**
- **Atualização para cadastramento e ativação do Pix.**

E, independente do motivo do contato, nunca pediremos:

- **Suas senhas;**
- **Código token;**
- **Códigos recebidos por SMS.**

Também não pediremos que digite esses dados em sites ou iremos transferir você para digitar esses dados em algum atendimento eletrônico. Se receber esse tipo de contato, não forneça nenhuma informação, desligue imediatamente e contate sua cooperativa.

Essas informações são confidenciais e devem ser utilizadas apenas para realizar suas operações financeiras nos canais oficiais do Sicredi.

Golpes por WhatsApp

Como acontecem:

Nesse golpe, golpistas **clonam o WhatsApp da vítima e utilizam sua foto e nome para aplicar golpes**. Eles se passam por atendentes de serviços de compra online ou por familiares e conhecidos da vítima, alegando que mudaram de número e precisam de ajuda urgente para resolver um problema. Com acesso à conta, os golpistas enviam mensagens aos contatos mais próximos da vítima, pedindo dinheiro emprestado.

Como se proteger!

A forma mais simples e eficaz de evitar que o WhatsApp seja clonado é ativando a opção **Verificação em duas etapas**.

Acesse: **Configurações/Ajustes > Conta > Verificação em duas etapas**

Com isso, você cria uma senha que será solicitada periodicamente pelo aplicativo, aumentando a segurança da sua conta.

Como se proteger!

Para evitar que sua foto seja utilizada indevidamente, você pode configurar para que ela seja **visível apenas para seus contatos salvos**. Esse cuidado vai evitar que golpistas usem a sua imagem e se passem por você para enganar seus conhecidos. É simples ativar essa opção:

iOS: no WhatsApp, acesse Ajustes > Conta > Privacidade > Foto de perfil > Meus contatos

Android: no WhatsApp, acesse Menu > Configurações > Conta > Privacidade > Foto de perfil > Meus contatos

Se alguém pedir dinheiro emprestado, é importante **ligar para confirmar se é realmente essa pessoa**, mesmo que a foto do contato seja de quem você conhece.

Nunca forneça o código de confirmação recebido por SMS para outras pessoas. Nem no WhatsApp, nem em nenhum outro aplicativo. Essa é uma dica que vale para todos os ambientes digitais.

Golpes de Phishing

Como acontecem:

Phishing vem do inglês “fishing” (pescar) e é usado para descrever tentativas de **enganar pessoas e “fisgar” informações pessoais.** Esses golpes tentam roubar suas senhas e dados pessoais ou bancários, como número de cartão, validade, código de segurança e códigos enviados por SMS.

Golpe do bloqueio de conta:

O golpista envia um falso e-mail ou SMS sobre bloqueio de conta em nome da instituição financeira informando possíveis irregularidades em seu cadastro, ou pedindo uma atualização dele, que pode levar a conta ao bloqueio total.

Golpe da atualização cadastral ou atualização de segurança:

O golpista envia um e-mail ou SMS com link, em nome da instituição financeira, informando a falta de atualização ou sincronização do código pedindo senhas e informações pessoais. A vítima é direcionada para um formulário ou página falsa que captura os dados da vítima para o golpista usar posteriormente.

Golpe do SMS com link:

Esse golpe é praticado com o envio de um link malicioso por SMS, direcionando a vítima para um formulário ou página que pedirá dados pessoais e bancários, como: senhas, códigos de segurança, números de cartões, entre outros. Por isso, é preciso ter atenção redobrada com esse tipo de mensagem.

Como se proteger!

Desconfie de promoções imperdíveis. Ao receber anexos por e-mail ou mensagem por WhatsApp, mesmo que o remetente seja conhecido, é importante verificar se existe aviso sobre extensões que precisam ser ativadas. Cuidado redobrado em páginas desconhecidas ou suspeitas (observar sempre a URL).

Cuidado com SMS suspeitos. Não clique em links com promoções suspeitas e não forneça dados pessoais ou senhas.

Cuidado com mensagens recebidas via WhatsApp ou Telegram. Elas também podem ser maliciosas e trazer conteúdos semelhantes aos enviados por e-mail ou SMS.

Não clique em links desconhecidos. Mesmo em campanhas solidárias divulgadas durante a pandemia ou outras causas sociais, desconfie de formulários que pedem seus dados — especialmente se você os recebeu por redes sociais ou por contatos conhecidos. Sempre verifique a fonte antes de interagir.

Para identificar um **e-mail suspeito**, verifique se o nome do remetente corresponde ao endereço de e-mail. Desconfie de erros de ortografia, logotipos borrados, pedidos de dados pessoais e mensagens com senso de urgência. URLs estranhas e anexos com formatos incomuns também são sinais de alerta.

Lembre-se sempre de que a forma ideal para acessar um site é digitando o endereço (URL) diretamente no navegador.

Sicredi | Pioneira desde 1902

Voltar ao menu

Golpes de Sites Falsos

Como acontecem:

Com a popularização da internet, as compras online se tornaram cada vez mais comuns. No entanto, muitos usuários ainda não verificam a autenticidade dos sites nem os requisitos básicos de segurança para garantir uma navegação segura. Esse descuido abre espaço para golpes envolvendo páginas falsas. **Golpistas criam um site quase idêntico ao verdadeiro com promoções tentadoras**, trazendo produtos com descontos fora do comum. Para dar credibilidade a farsa, se valem de marcas conhecidas e sérias.

Como se proteger!

- **Faça uma pesquisa de mercado comparando preços**. Desconfie se o valor for muito baixo.
- **Confira o endereço (URL) do site em que está comprando**. Sites falsos possuem domínios bastante similares aos verdadeiros. Dê preferência a sites cujos domínios terminam em .com.br
- **Não clique em links que levem direto aos sites de compras**. Esses sites podem ser falsos e conter vírus capaz de copiar dados sigilosos.
- **Localize o cadeado do navegador**: um site seguro apresenta o desenho de um cadeado ao lado da URL (endereço do site). Ao clicar nele, será exibido o certificado de segurança.

Voltar ao menu

Golpes do Boleto Falso

Como acontecem:

Esse golpe é cada vez mais comum e costuma acontecer por e-mail, mas também pode chegar por redes sociais, WhatsApp ou sites falsos. Ele se aproveita da confiança do consumidor em empresas com as quais já tem alguma relação.

O cliente recebe um boleto verdadeiro referente a uma compra ou serviço contratado. Pouco depois, chega um novo e-mail com outro boleto — desta vez com valor menor — alegando um erro no cálculo de impostos ou a concessão de um desconto especial.

Acreditando que a nova cobrança é oficial, a vítima realiza o pagamento. No entanto, com o passar dos dias, percebe que a empresa continua cobrando o valor original. É aí que descobre que caiu em um golpe: o dinheiro foi enviado para uma conta do golpista.

Esses boletos falsos são visualmente parecidos com os verdadeiros, mas contêm alterações na linha digitável, aquele código numérico usado para identificar o pagamento. Os golpistas modificam esses dados para que o valor vá para contas bancárias de terceiros ou dos próprios criminosos.

Como se proteger!

Observe se os seus dados (nome, CPF, endereço) que constam no boleto estão corretos e se há algum erro de português ou de formatação.

Verifique se os últimos números do código de barras correspondem ao valor do documento.

Fique atento a descontos e promoções inesperadas. Na dúvida, ligue para a empresa e confirme o valor e demais dados do documento.

Opte por pagar o boleto **utilizando o leitor do código de barras** disponível no aplicativo.

Ao fazer a leitura do código de barras, **verifique se o nome do beneficiário é realmente da empresa/pessoa contratada**.

Ao necessitar emitir uma segunda via de boleto, **faça o download do boleto diretamente no site da empresa** credora, utilizando uma conexão segura. Evite utilizar Wi-Fi público.

Em caso de suspeita, sempre **entre em contato com a empresa** para confirmar a legitimidade do boleto.

Sicredi | Pioneira desde 1902

Voltar ao menu

Engenharia Social

O que é Engenharia Social?

Engenharia social é uma técnica usada por golpistas para **enganar pessoas e levá-las a divulgar informações confidenciais**, como senhas e dados bancários, ou a clicar em links maliciosos que instalam vírus no dispositivo.

Diferente do que muitos pensam, esses golpes não exigem tecnologia avançada, apenas manipulação psicológica. O criminoso finge ser alguém confiável para convencer a vítima a ignorar medidas básicas de segurança.

Exemplo comum de golpe:
Um golpista se passa por funcionário de um banco e liga dizendo que é preciso atualizar o sistema. Ele pede que a vítima acesse um link e forneça dados pessoais, como senhas e números de conta.

Nenhuma instituição financeira realiza esse procedimento.

O Sicredi entra em contato com seus associados, **PORÉM não solicita:**

- Atualização do módulo de segurança.
- Atualização para ativação ou teste de Pix.
- Acesso a senhas, códigos bancários.
- Acesso ao aplicativo com dados pessoais.
- Atualização de dispositivos.
- Acesso a códigos recebidos por SMS ou e-mail.

Seguindo essas dicas e cuidados, você vai ficar muito mais protegido e pronto para orientar associados, amigos e familiares.

Avise amigos e familiares.

Compartilhe essa cartilha com todo mundo!

Assim, você ajuda outras pessoas a se protegerem e evitarem cair em golpes!

Sicredi | Pioneira desde 1902

Se precisar, entre em contato com a gente!

Nossos canais oficiais são:

SAC: informações, elogios e reclamações
0800 724 7220

WhatsApp
(51) 3358 4770

Atendimento às pessoas com deficiência auditiva ou de fala
0800 724 0525

Ouvidoria e Denúncias
0800 646 2519

Gerente: **contate diretamente o seu gerente de conta**

Sicredi | Pioneira desde 1902

Sicredi | Pioneira desde 1902