Proteja-se contra golpes e fraudes.

GUIA DE PREVENÇÃO

escolha segurança.

UNICRED

01 OBJETIVO DA CARTILHA

Olá Cooperado(a)

O objetivo dessa cartilha é conscientizar quanto ao uso dos canais digitais e não digitais, além de trazer mais conhecimento em relação aos tipos de golpes e dicas de prevenção.

Juntos podemos construir uma essência colaborativa no repasse de conhecimento.

Vamos aprender!

02 PROTEJA SUAS SENHAS

_Nunca informe a terceiros suas senhas ou códigos recebidos em seu celular via SMS.

_Troque suas senhas periodicamente e lembre de criar combinações fortes.

COMO CRIAR UMA SENHA FORTE?

Senhas com oito ou mais caracteres alfanuméricos.

Utilize letras, números e caracteres especiais.

EX: C@m1LaS0uZa

Evite acessar sua conta em computadores ou redes Wi-Fi públicas. Garanta que ninguém esteja te observando no momento de incluir suas senhas (caixa eletrônico, maquininha de cartão, computador, etc).

FIQUE ATENTO

A Unicred NÃO entra em contato solicitando: senhas, número de cartão ou informações pessoais.

Lembre-se: sua senha é única e intransferível, NÃO compartilhe!

03 ACESSE SUA CONTA DE FORMA SEGURA

UNICRED MOBILE

_Em caso de perda ou roubo de celular, entre em contato imediatamente com a sua cooperativa.

_Se perceber algum processo ou comportamento fora do comum durante o seu acesso no aplicativo, tome cuidado. Seu dispositivo pode estar infectado com itens maliciosos.

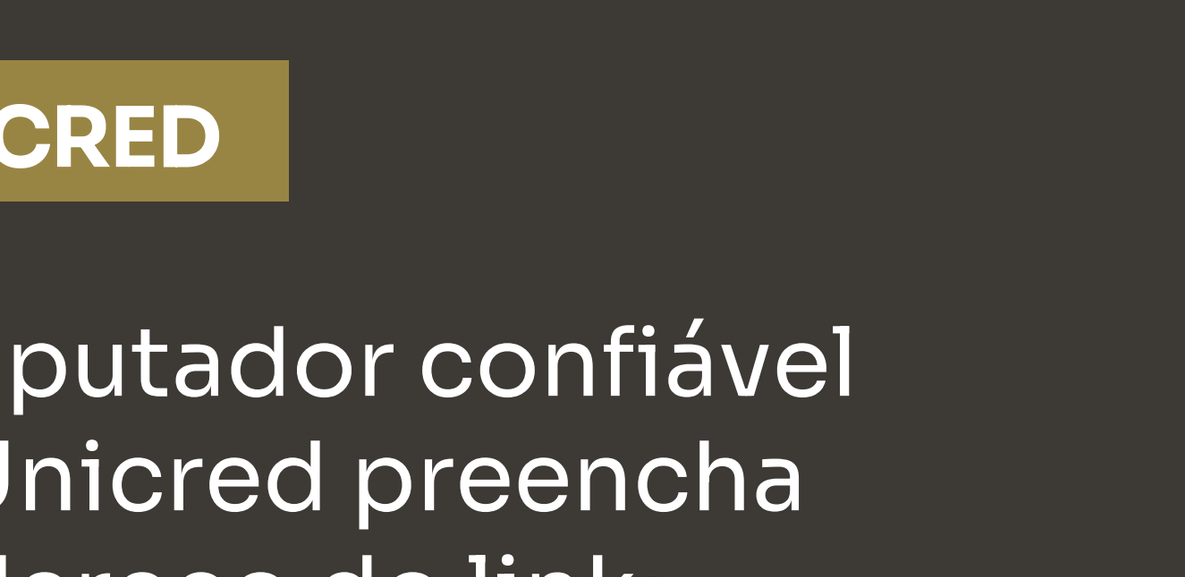
_Caso receba algum e-mail, SMS ou mensagem solicitando o reenvio do token ou senha de acesso, NÃO forneça as informações. Entre em contato imediatamente com a Unicred e reporte a situação.

_Fique atento caso seu celular fique inoperante sem motivo aparente. Você pode ter sido vítima de um roubo de linha.

INTERNET BANKING UNICRED

Sempre utilize um computador confiável e ao acessar o site da Unicred preencha o site completo no endereço do link:

unicred.com.br



Lembre-se: nunca utilize celulares de terceiros para acessar a sua conta e mantenha seu antivírus atualizado.

03 ACESSE SUA CONTA DE FORMA SEGURA

CAIXA ELETRÔNICO

_Esteja atento à aproximação de estranhos enquanto utiliza um caixa eletrônico.

_Caso seu cartão fique retido em um caixa eletrônico, não aceite ajuda de estranhos.

_Não abandone o caixa eletrônico antes de concluir e encerrar a operação.

_Fique sempre em alerta ao utilizar o caixa eletrônico.

CHEQUE

_Guarde seus cheques sempre em local seguro.

_Em caso de perda, furto ou roubo de cheques, entre em contato imediatamente com a Unicred.

_Mantenha seu cadastro na Unicred atualizado, de forma que possamos agilizar o contato e confirmar suas informações em caso de dúvidas.

_Descarte de maneira correta os talões e folhas de cheques de contas encerradas.

_Não permita que outras pessoas preencham seus cheques.

Para mais informações, entre em contato com a Unicred ou com seu Gerente de Relacionamento.

03 ACESSE SUA CONTA DE FORMA SEGURA

CARTÃO

_Sempre mantenha o seu cartão em local seguro e nunca o perca de vista.

_Seu cartão de débito ou crédito é pessoal e intransferível. Nunca empreste ou revele a senha para terceiros.

_Nunca entregue o seu cartão bancário para terceiros ou estranhos, ainda que só por alguns instantes.

_Ao comprar com seu cartão pela internet ou telefone, certifique-se da veracidade da empresa.

_Confira o valor da transação antes de colocar a senha para pagamento. Se tiver dúvida ou não estiver visível, não digite a senha.

_Nunca deixe que vejam a sua senha na hora de digitar.

_Verifique se o cartão é o seu após cada transação e sempre coloque e retire você mesmo da máquina de pagamento.

_Se não reconhecer algum lançamento em sua fatura, entre em contato com a Central de Relacionamento.

_Bloqueie o seu cartão imediatamente em caso de perda ou roubo e acione a Central de Relacionamento.

03 ACESSE SUA CONTA DE FORMA SEGURA

PIX

_Realize o PIX somente em dispositivos confiáveis e cadastrados com a sua conta da Unicred.

_Sempre verifique o destinatário que irá receber a transferência.

_Em caso de um pedido incomum de transferência de dinheiro via aplicativo de mensagem, sempre confirme com a pessoa por outros canais de comunicação a veracidade da informação.

04 FUJA DOS GOLPES

O que é a Engenharia Social?

Engenharia Social é um método de ataque que utiliza a persuasão, aproveitando-se na maioria das vezes da ingenuidade, confiança e boa-fé das vítimas para obter informações sigilosas e que podem lesar a pessoa ou seus conhecidos.

Vamos entender alguns tipos de golpes para não cair nessa cilada!

GOLPE DO FALSO COLABORADOR

_Um terceiro liga se passando pela Instituição Financeira. Durante a ligação, informa que é necessário efetuar atualizações de segurança e orienta a vítima a acessar um link.

_O link direciona a vítima para um site falso, muito semelhante ao da Instituição Financeira.

_A vítima, achando que se trata de um site verdadeiro, acaba disponibilizando suas informações: conta, usuário, senhas e Unitoken.

_Tendo acesso às informações, o terceiro entra na conta da vítima e efetua transações sem o seu consentimento.

Lembre-se: sua Instituição Financeira NUNCA entrará em contato solicitando informações pessoais.

GOLPE DO WHATSAPP

_Um terceiro acessa informações pessoais obtidas nas redes sociais ou no próprio WhatsApp da vítima.

_Com isso, cria uma conta falsa no WhatsApp e começa a solicitar dinheiro para o grupo de amigos da vítima.

Lembre-se: não disponibilize suas informações pessoais em redes sociais, qualquer pessoa pode ter acesso a elas.

GOLPE COMPRA/VENDA DE MERCADORIA

_O golpista cria um anúncio falso em uma plataforma de compra e venda.

_A vítima se interessa pelo produto com o preço vantajoso e pede mais informações ao "vendedor".

_O golpista solicita que a vítima entre em contato pelo WhatsApp para facilitar a comunicação.

_Por fim, o golpista informa que o produto já possui vários interessados e solicita a vítima uma entrada do pagamento para “garantir” a venda do produto.

Não caia nessa: desconfie de ofertas abaixo do valor de mercado, além disso, pesquise informações da pessoa com quem está negociando.

GOLPE DO EMPRÉSTIMO FALSO

_Os golpistas fazem anúncios ofertando empréstimos em condições vantajosas, se passando pelas Instituições Financeiras.

_Após contato da vítima, os criminosos solicitam o pagamento de uma taxa para realizar a liberação do empréstimo.

_São solicitados vários pagamentos até a vítima entender que se trata de um golpe.

GOLPE DO FALSO MOTOBOY

_Os golpistas ligam para a vítima informando que há transações suspeitas em seu cartão.

_Na ligação, são confirmados os dados pessoais da vítima e é solicitado para digitar a senha do cartão.

_Por fim, é informado que será enviado um motoboy para coletar o cartão e que é necessário cortá-lo ao meio, mas sem danificar o chip.

Lembre-se:
nenhuma Instituição irá até sua residência para coletar seus cartões.

GOLPE DA FALSA LOJA VIRTUAL

_Os golpistas criam uma página falsa, praticamente idêntica a de uma loja real, anunciando produtos com valores muito abaixo do preço de mercado.

_As vítimas inserem os dados do cartão que posteriormente são utilizados em compras fraudulentas.

Para se prevenir:
verifique se o endereço (URL) é o oficial da loja e suspeite de preços muito baixos.

GOLPE DO INSTAGRAM

Neste golpe é possível identificar dois tipos de atuações mais comuns:

_O fraudador clona o perfil do Instagram e anuncia venda de produtos com preço abaixo do mercado, geralmente informando que está de mudança.

_O fraudador faz um anúncio no Instagram de um produto atrativo, seleciona o nicho de pessoas que deseja atingir e realiza a venda do produto, porém a mercadoria nunca é entregue e assim a vítima identifica que caiu em um golpe.

Importante: Valide as informações em ambas as situações. No caso de anúncios de venda no Instagram de um amigo, tente contato por outro canal (WhatsApp, por exemplo) para confirmar a veracidade. Já no caso da loja virtual falsa, pesquise sobre a loja ou perfil antes de finalizar a compra.

GOLPE DA TROCA DO CARTÃO

_Os golpistas se passam por vendedores ambulantes ou falsos funcionários (principalmente em eventos, lojas, em locais turísticos, entre outros) e se aproveitam da distração das vítimas.

_No momento da compra, eles memorizam a senha enquanto a vítima digita na máquina de cartão. Após a retirada do cartão da máquina sem que a vítima perceba, os golpistas trocam o cartão por outro. De posse do cartão e da senha memorizada, os fraudadores fazem compras e saques no cartão da vítima.

GOLPE SIM SWAP

Fraudadores assumem
o controle das contas
de celular de suas vítimas.

Como funciona?

_O fraudador coleta dados da vítima (através de mídia social, vazamento de dados, phishing etc) e, com essas informações, se passa pela vítima para entrar em contato com a operadora de telefonia (pessoalmente ou remotamente).

_A partir daí, o criminoso tem acesso às suas ligações, mensagens e senhas, podendo ativar aplicativos em outro aparelho. Com os app ativos, o fraudador pode acessar suas contas em instituições financeiras para desviar valores, realizar empréstimos, ou aplicar outros golpes.

Algumas dicas para se proteger:

_Evite usar verificação em duas etapas via SMS, desta forma o fraudador receberá o código de liberação se estiver com acesso ao seu número;

_Ative os códigos PIN do seu chip SIM, ele será necessário ao inserir o chip com seu número em um novo celular ou reiniciar o aparelho;

_Utilize senhas fortes e únicas para cada conta online, considere o uso de um gerenciador de senhas para ajudar a proteger suas informações de login;

Fique atento: Na perda total do sinal do seu celular sem motivo aparente, entre em contato com sua operadora para verificar a situação e solicite o bloqueio imediato do número para evitar perdas.

GOLPE BOLETO FALSO

_A vítima realiza a emissão da segunda via do boleto em um site fraudulento, fazendo com que o beneficiário do pagamento seja o fraudador.

_Também pode ocorrer da vítima estar com o computador infectado por um malware que adultera a linha digitável do boleto, fazendo com que o beneficiário do pagamento seja o fraudador.

Atenção: Sempre observe antes de finalizar a transação se o beneficiário do boleto está de acordo com o original. Caso verifique que o beneficiário está divergente no comprovante de pagamento, contate seu gerente imediatamente para que possa ser realizada a tentativa de recuperação junto à instituição beneficiária.

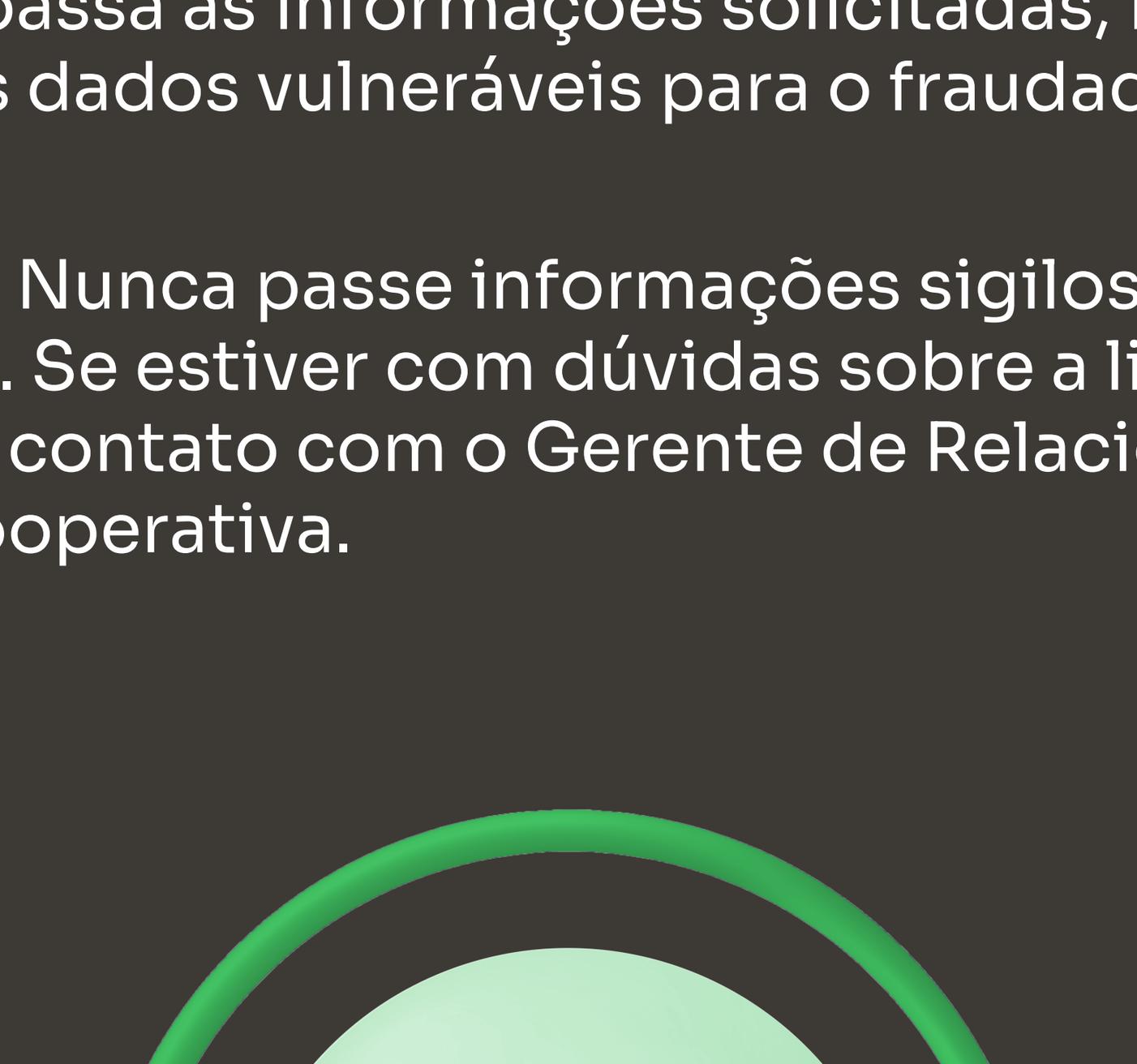
GOLPE CENTRAL FALSA

_O fraudador entra em contato com a vítima informando ser da Central de Atendimento do banco e indica algumas transações indevidas em sua conta, pedindo que a vítima entre em contato através do número que consta no verso do cartão.

_A vítima entra em contato com o número da Central de Atendimento verdadeira, no entanto o fraudador utiliza a técnica de ID Spoofing para que esta ligação seja direcionada para ele.

_Com a credibilidade de estar ligando para o número correto da Central de seu banco, a vítima passa as informações solicitadas, ficando com seus dados vulneráveis para o fraudador.

Atenção: Nunca passe informações sigilosas para terceiros. Se estiver com dúvidas sobre a ligação, entre em contato com o Gerente de Relacionamento da sua cooperativa.



GOLPE TABELA PIX

_O golpista divulga via redes sociais, geralmente hackeadas de pessoas conhecidas, uma tabela de transferência PIX onde a vítima supostamente pode receber até cinco vezes o valor investido.

Importante: Não existe investimento com esse tipo de retorno. Fique atento.

GOLPE DO FALSO EMPREGO

_Golpistas induzem as pessoas a clicarem em links ou preencherem informações pessoais afim de roubar dados bancários, CPF, telefone, entre outros. Além disso, podem solicitar valores em troca de prêmios ou brindes.

Cuidado: Não forneça seus dados pessoais em redes sociais, WhatsApp ou links suspeitos, pois eles podem ser utilizados por criminosos. Desconfie sempre.

GOLPE DO INVESTIMENTO

_Golpistas entram em contato com as vítimas, normalmente por redes sociais hackeadas, com ofertas de investimento em criptomoedas, minérios, entre outros, ofertando ganhos altos e imediatos.

Atenção: Não existe investimento com retorno rápido e alto. Pesquise antes.

O QUE DEVE SER FEITO SE CAIR EM UM GOLPE?

1_ Busque contato imediato com a Instituição Financeira pela qual a operação foi feita e explique todo o ocorrido.

2_Registre um boletim de ocorrência policial, fornecendo o máximo de informações, para que ocorra uma investigação.

3_Caso tenha sido vítima de clonagem de WhatsApp, é necessário reportar essa situação para o contato support@whatsapp.com, solicitando a desativação temporária de sua conta.

4_Habilite o fator em duas etapas, isso impede que o golpista faça a clonagem do WhatsApp.

COOPERADO(A): fique atento e evite cair em golpes. Caso perceba algo suspeito, procure a Polícia ou a sua Instituição Financeira.

05 DICAS DE SEGURANÇA

_A Unicred NÃO entra em contato com os seus Cooperados solicitando informações pessoais.

_Tenha sempre um antivírus atualizado em seus dispositivos.

_Em aplicativos, habilite a verificação em duas etapas.

_Evite acessar e-mails, SMS e páginas desconhecidas.

_Não forneça códigos ou responda solicitações de atualização cadastral.

_Desconfie de mensagens incomuns, com pedidos de socorro, mensagem com erros gramaticais ou ofertas imperdíveis.

_Identificou algo suspeito em sua conta Unicred?

ENTRE EM CONTATO IMEDIATAMENTE
EM NOSSOS **CANAIS OFICIAIS**

0800 200 7302 (WhatsApp)
3003 7703 (capitais e regiões metropolitanas)
0800 200 7302 (demais cidades)

UNICRED - INSTITUIÇÃO FINANCEIRA COOPERATIVA

A Unicred tem como objetivo estar sempre ao seu lado com as melhores soluções financeiras para uma experiência diferenciada.

escolha segurança.

UNICRED