Golpes e fraudes

tudo que você precisar saber

CRESOL

Fique atentento(a)

Com tantas ameaças e pessoas de má-fé no ambiente online ou fora dele, fica difícil se proteger, não é mesmo? O número de golpes cresce ano após ano e com o surgimento de novas tecnologias, os criminosos desenvolvem métodos cada vez mais sofisticados, o que deixa milhares de pessoas vulneráveis.

Por isso, reunimos neste material os principais tipos de golpes para que você tenha conhecimento e possa identificar potenciais situações de risco.

A Cresol não entra em contato para pedir informações ou dados bancários por WhatsApp, ligação telefônica ou SMS.

Na dúvida, entre em contato com o seu gerente ou utilize algum canal de relacionamento Cresol informados no site oficial.

Sumário

WhatsApp clonado

O fraudador liga para uma vítima em potencial, e por da meio de engenharia social convence a vítima a informar o código que é enviado por SMS que habilita a conta no celular do golpista, que passa a utilizar do aplicativo de mensagens - WhatsApp, para ter acesso a lista de contatos da mesma, e se passando pela vítima, pede dinheiro emprestado, geralmente por uma transferência via PIX.

Como evitar:

• Se receber um código, não encaminhe o código para ninguém;
• Ative a autenticação de dois fatores nas configurações do seu WhatsApp.

Falso leilão

Empresa fraudulenta com objetivo de obter informações sensíveis, e a venda de veículos que não estão disponíveis. Geralmente o site solicita o pagamento antes do leilão acontecer e logo após o lance é enviado um boleto para pagamento. O arrematador é bloqueado assim que concluir o pagamento.

Como evitar:

• Desconfie de sites de leilões de veículos, residências e objetos com valores muito discrepantes, pesquise sobre o leiloeiro, não realize transferências antecipadas.
• Validar a veracidade da empresa confirmando se o domínio do site é brasileiro. Exemplo: nomedosite.**com.br**;
• Confira se o endereço existe e bate com a informação do site;
• Confirme o CNPJ da empresa no site da Junta Comercial do seu estado.

Falso intermediário

Ocorre geralmente na compra de veículos - quando uma terceira pessoa faz o contato entre o comprador e o vendedor, e apresenta propostas distintas a cada um, criando uma história por trás da compra, e dessa forma obtendo domínio sobre a negociação. O intermediário acaba recebendo o pagamento referente a venda e não realiza o repasse ao verdadeiro dono. Em golpes desse formato tanto o vendedor quanto o comprador podem sair lesados, logo que em alguns casos o veículo pode ser transferido ao comprador, porém o vendedor não recebe o devido pagamento.

Como evitar:

- Desconfie de ofertas muito vantajosas e terceiros falando em nome do dono;
- Verifique toda a documentação do automóvel;
- Não faça pagamentos antecipados.

Falso emprego

O golpe do falso emprego consiste em mensagens compartilhadas em redes sociais, SMS, anúncios publicitários e outros meios que afirmam que uma empresa está contratando funcionários com urgência. A pessoa é levada a fazer um cadastro, mas, no fim das contas, não recebe o emprego. A ação visa, na verdade, fazê-la pagar por um suposto curso ou taxa de inscrição, por exemplo, mas a vaga de trabalho em si não existe.

Como evitar:

- Desconfie quando houver uma taxa para se cadastrar;
- Confirme e-mail, número e nome da empresa da suposta vaga.

Falso colaborador Cresol

Ocorre quando o golpista está se passando por um colaborador Cresol e utiliza da engenharia social para obter dados sensíveis, informar débitos pendentes e cobranças indevidas. Para empresas, o golpista também pode informar contratos falsos em desacordo, repassam falsos contatos de empresas fantasmas, e cobram para regularização da situação, que caso não ocorra, a empresa terá o CNPJ bloqueado.

Como evitar:

• Confirme as informações com o seu gerente;
• Desconfie quando receber SMS, ligação ou contato via WhatsApp, a Cresol não entra em contato para pedir informações ou dados bancários.

Boleto fraudulento

O boleto falso pode ter distintas origens, como por exemplo e-mail, sites falsos, WhatsApp ou em meio físico. O golpista utiliza da engenharia social para justificar o boleto pendente, seja de uma compra, uma mensalidade ou quitação de débitos. Na maioria dos casos o golpista já tem o conhecimento de dívidas que a vítima possui, o que facilita a ação. Ocorre com grande frequência em empresas, logo que as movimentações financeiras diárias são maiores em comparação a uma pessoa física.

Como evitar:

• Confirme as informações do favorecido;
• Certifique-se, e valide sempre o emitente e a origem do meio a qual o boleto foi recebido

Golpe do bug

Nesse golpe, os criminosos espalham notícias de que o PIX está com alguma falha no funcionamento e é possível ganhar o dobro do valor transferido Na mensagem, os golpistas explicam que, para a ação dar certo, é preciso enviar dinheiro para chaves específicas e, em seguida, compartilham supostos números que funcionam. Só que quem resolve testar transferindo o dinheiro para as chaves informadas está, na verdade, mandando dinheiro para os golpistas.

Como evitar:

• Desconfie de proposta de ganho de dinheiro fácil e rápido.

QR code falso

Uma das formas de fazer pagamentos por PIX é via QR Code. Atualmente, é comum vermos QR Code para transferências em lives e apresentações online que arrecadam dinheiro para artistas ou instituições. Os golpistas fazem o download desses vídeos e criam uma nova transmissão com um QR Code falso, divulgam o vídeo e o dinheiro vai direto para a conta do criminoso.

Como evitar:

• Verifique sempre a conta corrente e nome do favorecido.

Comprovante de PIX Falso

O falso comprovante de PIX é um golpe operado em transações eventuais e informais entre desconhecidos, ou seja, quando ainda não está estabelecida uma relação de confiança entre as partes. É o caso de compra e venda entre pessoas

físicas quando há uma transação feita pela internet, mas com entrega física do produto.

O criminoso vai até o local combinado para a entrega, retira o produto e envia por WhatsApp um comprovante de transferência via PIX. O comprovante é idêntico ao gerado pelo banco, porém falso.

Como evitar:

• Verifique à instantaneidade da operação PIX. Se a transferência tiver sido feita, ela vai cair na hora na sua conta;
• Não aceite agendamento de PIX no caso de primeira venda. Uma dica é acionar as notificações nos aplicativos de instituições bancárias;
• Desconfie caso você tenha recebido o comprovante, mas não a notificação.

Falso agendamento PIX

O golpista forja um comprovante de transferência por meio de PIX de uma instituição bancária e envia para você por WhatsApp ou e-mail. Você estranha aquele comprovante de depósito e questiona ao que se refere. Neste momento, o criminoso explica que errou ao realizar o pix e pede que você reembolse o valor para a conta dele. Outra abordagem é do pix agendado. Neste caso, os infratores agendam uma transferência para a conta da vítima, acionam a vítima para avisar o erro e pedir reembolso. Quando a vítima transfere a quantia, os golpistas suspendem o agendamento.

Como evitar:

• Ao ser abordado por desconhecidos com comprovantes de PIX, esteja atento e antes de reembolsar espere a confirmação de compensação do valor na sua conta bancária;

• O PIX permite devolução de valores transferidos, basta clicar no valor creditado. Se efetivamente houver o erro na transferência, você poderá devolver por meio do aplicativo do banco mesmo;

• O Banco Central anunciou para novembro de 2021 a operacionalização de um mecanismo de devolução de valores nos casos de transações suspeitas. O reembolso poderá ser implementado pela própria instituição financeira desde que o correntista tenha o registro de boletim de ocorrência fundamentado. Por isso é importante reunir o máximo de provas e fazer o registro na polícia.

Golpe do motoboy

Nessa fraude, o golpista se identifica como colaborador da instituição através de uma ligação e alega que existem transações suspeitas em seu cartão. Logo em seguida coleta seus dados e avisa a necessidade de retirada do seu cartão físico por um motoboy em seu endereço.

Como evitar:

• Não passe seu endereço ou entregue o seu cartão a ninguém, nem mesmo se estiver danificado. A Cresol não envia motoboy para recolhimento de cartão;
• Caso desconfie da ligação, desligue o telefone entre em contato com sua agência, ou de preferência se dirija a agência da Cresol mais próxima.

Golpe do falso sequestro

O golpe do falso sequestro é aplicado de forma a obter ganho através de ameaças praticadas a uma vítima, informando que um membro de sua família se encontra refém.

Como evitar:

- Mantenha a calma ao receber esse tipo de informação;
- Verifique se a pessoa mencionada na ligação se encontra bem;
- Não passe nenhuma informação pessoal pelo telefone;
- Procure a segurança pública para registro de uma ocorrência.

Golpe do pacote de dinheiro

A prática dessa ação tem início com a vítima sendo observada e acompanhada pelo golpista. Ao realizar um saque e sair da agência com elevada quantia em dinheiro passa a ser seguida. Um deles deixa propositadamente cair uma folha de cheque de alto valor ou um pacote de dinheiro falso, chamando a atenção da vítima. Uma segunda pessoa envolvida no golpe, aproxima-se e confirma o acontecido, essa ação convence a vítima e também que os dois devem juntos devolver o dinheiro. Após a situação, o golpista que deixou cair o cheque ou dinheiro, agradece e oferece uma recompensa à vítima e ao comparsa, dizendo que eles deverão comparecer a um escritório, para receber a dita recompensa. O golpista vai receber a suposta recompensa e chama a atenção da vítima ao retornar com uma boa quantia em dinheiro. Na sua vez de receber a recompensa, a vítima é orientada a deixar seus pertences sozinhos, somente percebendo que tratava-se de um golpe quando os estelionatários já desapareceram com seus bens pessoais e seu dinheiro.

Como evitar:

- Não confiar em pessoas estranhas é a melhor maneira de evitar o golpe;
- Procurar transitar em locais seguros quando estiver com posse de alto valor de dinheiro;
- Seguir direto ao local desejado com o valor do saque, evitar distrações no percurso;
- Jamais informe para outras pessoas a data e horário que será realizada a retirada do dinheiro;

Golpe da maquininha quebrada

Este golpe é aplicado principalmente em serviços de entrega de comida por delivery. O golpista utiliza a desculpa que o visor da maquininha de cartão está quebrado ou danificado, aproveitando da situação realiza a cobrança com um valor maior do que seria o pagamento.

Como evitar:

• Realizar pagamentos através dos aplicativos de entrega;
• Cobranças adicionais no momento da entrega não devem ser pagas;
• Pagamentos em maquininhas com visor quebrado ou danificado devem ser negados;
• Utilize o recurso de serviços de SMS para receber notificações de pagamentos com seu cartão.

Clonagem de cartão no ATM - chupa cabra ou anti skimming

O meliante insere um equipamento junto ao terminal de autoatendimento, caixa eletrônico, um equipamento que efetua a leitura dos dados do cartão e armazena, e posteriormente coletam esses dados e gravam em um cartão virgem, completando a clonagem do cartão.

Como evitar:

• Ficar atento a qualquer situação diferente no equipamento, como por exemplo a dificuldade para inserir ou retirar o cartão do ATM;
• Ficar atento também ao extrato de utilização do cartão, e em caso de alguma movimentação não reconhecida, solicitar o bloqueio do cartão com urgência;

• Atentar-se para qualquer alteração visual que possa existir no equipamento, como por exemplo, cores diferentes, falta de assimetria e possíveis “pedaços” soltos do ATM, ressaltos no local de leitura de códigos de barras.

Golpe das falsas centrais

Alguns golpistas procuram entrar em contato com os clientes se passando por empregados das centrais de cartões ou do banco, para obter informações e, assim, aplicar golpes.

Como evitar:

• As verdadeiras Centrais de Segurança dos Cartões podem entrar em contato com você para confirmar transações e/ou alterações cadastrais realizadas no cartão de crédito, porém NUNCA pedem senha ou o número completo do cartão. Podem ser solicitados APENAS os quatro últimos dígitos.

Golpe do “como posso ajudar?”

O golpista aborda pessoas com dificuldades nos caixas eletrônicos fingindo auxiliar nas transações e trocam o cartão e/ou realizam transações espúrias nas contas das vítimas.

Como evitar:

• Não aceite ajuda de estranhos nos caixas eletrônicos e em caso de dificuldades solicite a ajuda de um funcionário da agência devidamente identificado ou o auxílio de uma pessoa de sua confiança.

Bilhete premiado

O golpista aborda a vítima e diz que possui um bilhete premiado, mas que não pode receber todo o prêmio, pois sua religião não permite e que para receber o prêmio, precisa de duas testemunhas. Nisso, um comparsa se aproxima e o golpista exige da vítima certa quantia em dinheiro para demonstrar boa-fé e a vítima, acreditando na história, vai à agência e saca o dinheiro, uma vez que o comparsa também repassa o dinheiro ao golpista. Com o dinheiro em mãos, ele usa uma desculpa e desaparece, geralmente está bem vestido, em um carro bom e conversa bem.

Como evitar:

• Diga que não tem interesse e saia de perto.

PIX Premiado

O golpe é divulgado livremente nas redes sociais. Em troca de um depósito inicial com valor baixo é prometida uma oferta de altos valores de volta. Os criminosos usam contas de pessoas que perderam acesso às redes sociais, ou seja, contas hackeadas.

Como evitar:

Desconfie de promessas na internet. Todo mundo gosta de ter um bom retorno financeiro. Confira bem quem está pedindo dinheiro. Muitas vezes, os golpistas podem até pedir transferências por PIX se passando por alguém que você conheça. Somente realize uma transferência por PIX se você tiver certeza do destinatário e se for uma pessoa da sua real confiança.

Golpe do falso familiar

Maior incidência de Golpes

O golpista geralmente cria um perfil falso no aplicativo WhatsApp com a foto do usuário e passa a conversar com parentes e amigos se passando pelo usuário fingindo que trocou de número e solicitando que atualize o contato. Em seguida, solicita empréstimos de emergência geralmente via transações PIX ou TED usando desculpas para justificar a solicitação.

Como evitar:

Sempre desconfie de pessoas próximas solicitando auxílio financeiro, para transferências via PIX, TED, pagamentos de boletos e outros. Se receber um código, não encaminhe o código para ninguém. Ative a autenticação de dois fatores nas configurações do seu WhatsApp.

Cuidados que você precisa ter.

Confira algumas dicas em relação a criação de senhas e atitudes indicadas na hora de ir a um caixa de autoatendimento.

fique mais seguro

Cuidados com senhas

Sua senha é pessoal, inequívoca e intransferível. Jamais revele sua senha a terceiros, nem mesmo para um colaborador da Cresol ou para alguém de sua confiança.

Ninguém está autorizado a solicitar sua senha em nome da Cresol, seja por telefone, email ou até mesmo presencialmente na agência.

Quando estiver digitando sua senha, verifique se não existe alguém **observando a digitação**.

Memorize sua senha, evite anotar em papel, nem a deixe armazenada em seu computador, celular ou dispositivos móveis de armazenamento. E jamais deixe-a junto ao cartão.

Ao **criar uma senha**, não utilize em sua composição, data de nascimento, telefones, números de documentos, placa de automóvel ou sequências de teclas do computador (exemplo: "123456", "qwerty", "asdfghjkl" etc.). Combine números, símbolos e letras maiúsculas e minúsculas.

Não digite suas senhas em sites desconhecidos, ou em páginas abertas através de links recebidos por e-mail, SMS ou Whatsapp.

Altere regularmente suas senhas. Se suspeitar que sua senha foi comprometida, troque-a imediatamente.

Evite repetir senhas usadas anteriormente, busque sempre uma senha nova.

Atitudes seguras no autoatendimento

- Antes de entrar em salas de autoatendimento **verifique se não há pessoas suspeitas** dentro do ambiente.
- Ao utilizar os caixas eletrônicos, posicione-se de maneira a **encobrir o teclado com o próprio corpo**, para evitar que alguém visualize a digitação dos dados.
- **Nunca forneça sua senha** para outra pessoa.
- Antes de sair do autoatendimento após um saque, **guarde o dinheiro em local seguro.**
- **Problema com seu cartão, use o seu telefone para contato** com a central de atendimento.
- Se precisar de ajuda, **verifique se os funcionários estão devidamente identificados.**
- Não ceda, não empreste e não deixe **ninguém pegar o seu cartão.**
- Não use caixas eletrônicos que apresentem **sinais de vandalismo.**
- **Nunca aceite ajuda de estranhos,** não permita que se aproximem quando estiver utilizando um caixa eletrônico.
- Após utilizar o caixa eletrônico, **confira se o cartão que está guardando é o seu para não cair no golpe da troca do cartão.** Geralmente, a troca por outro cartão ocorre quando lhe oferecem ajuda, ou esbarrando em você propositalmente para que seu cartão caia e o fraudador consiga rapidamente trocá-lo por outro.

Cuidados

Nunca forneça a senha do cartão a estranhos. Pessoas mal intencionadas podem oferecer ajuda ou puxar conversa quando você estiver utilizando a sala de autoatendimento.

Nunca aceite propostas, como a transferência de valores para sua conta, tampouco o uso da sua conta por terceiros para transações que não são de seu interesse.

Sempre clique em "sair" pois uma das tentativas de golpe acontece quando alguém pede para você voltar ao caixa eletrônico dizendo que sua sessão não foi encerrada. Nesse momento, o fraudador pede que você insira novamente sua senha no teclado físico ou mesmo em uma tela aberta por ele, onde a senha aparece em texto claro, em vez de asteriscos. Para evitar essa cilada, ao terminar de fazer suas operações, sempre aperte a tecla "Sair". **Ao deixar o caixa eletrônico, se alguém pedir para você voltar, não volte.**

Quando for fazer saques ou depósitos em caixas eletrônicos ou agências, **fique atento às pessoas que estão ao redor.** Criminosos costumam observar os clientes para identificar aqueles que efetuam retiradas elevadas nos guichês ou terminais de autoatendimento. Ao sair da agência, você pode ser seguido e abordado por um deles, que exigirá a entrega do dinheiro. Algumas vezes, eles sabem até dizer o valor que sacou e o local onde você guardou o dinheiro. Esse crime é conhecido como "golpe da saidinha".

À noite, redobre o cuidado e evite usar os caixas de autoatendimento. Nesse período, a circulação de pessoas diminui e você fica mais exposto a riscos.

Evite ir sozinho em terminais de autoatendimento ou em instituições financeiras com terminal 24 horas e de preferência em horários de maior movimento.

Cuidados na Saída da Agência

- **Verifique** se ao sair alguém não lhe segue.
- **Olhe** para todos os lados.
- **Evite efetuar movimentação durante períodos de pouca luminosidade** externa, pois acarreta em maior risco por não ter visualização clara.
- **Evite ao máximo efetuar saques de alto valor**, opte por transferências ou PIX.
- **Ficar atento a veículos suspeitos** que possam estar parados em frente a agência, principalmente se identificar que existem pessoas no interior do mesmo.

Ficou com dúvidas ou precisa falar conosco?

Ouvidoria / SAC / Denúncia

0800 643 1981
Segunda a Sexta,
08h30 às 11h00
12h30 às 17h00

Cartões Cresol

4007 1600 - Regiões Metropolitanas
0800 704 7500 - Demais regiões

Dúvidas sobre segurança:
cresol.com.br/seguranca


CRESOL