



USO CONSCIENTE DO PLANO DE SAÚDE

Dicas de prevenção à fraude e utilização
adequado dos serviços de saúde

Unimed 
Fesp

ANS Nº 319996

PALAVRA DA DIRETORIA EXECUTIVA

Cumprindo o principal objetivo do Programa de Integridade da Unimed Fesp, que é promover a ética e a integridade no ambiente de negócios, elaboramos esta cartilha para esclarecer e alertar nossos clientes e parceiros comerciais sobre os danos causados pelas fraudes, que impactam a sustentabilidade de todo o sistema de saúde.

A fraude na operação de planos de saúde ocorre quando informações falsas são fornecidas ou omitidas para obter algum tipo de vantagem ou recursos financeiros de forma ilegal. Ela pode ser praticada por beneficiários (usuários do plano de saúde), profissionais e estabelecimentos de saúde, além de corretores e administradores que intermedeiam a venda de planos de saúde. Algumas práticas, que podem ser consideradas inofensivas ou comuns, como o fracionamento de recibos para obtenção de reembolsos, são, na verdade, crimes passíveis de punição conforme a lei.

O mau uso do plano de saúde resulta no aumento dos custos dos procedimentos, seja por fraudes ou pela realização de procedimentos desnecessários e repetitivos, o que acaba sendo repassado aos beneficiários por meio do aumento das mensalidades para cobrir os prejuízos. Além disso, isso pode causar uma diminuição nas opções de profissionais e estabelecimentos de saúde disponíveis.

O uso responsável do plano de saúde e a conscientização de todos os envolvidos sobre a importância da integridade nesse relacionamento são fundamentais para manter o equilíbrio de todo o sistema de saúde do país. Nossa expectativa é que esse material seja útil para aumentar o conhecimento sobre as diversas modalidades de fraudes e, com esse conhecimento, o cliente Unimed esteja mais precavido para evitar esses transtornos. Aproveite a leitura!

Diretoria Executiva
Federação das Unimeds do Estado de São Paulo (Unimed Fesp)

INTRODUÇÃO

Você sabia que, anualmente, estima-se que as operadoras de planos de saúde gastem entre R\$ 30 bilhões e R\$ 34 bilhões (dados do IESS – Instituto de Estudos de Saúde Suplementar, de 2023, referente ao ano 2022) para cobrir custos de procedimentos médicos desnecessários, desvios e irregularidades em contas hospitalares?

Esses valores prejudicam diretamente os beneficiários de planos de saúde, as operadoras e todos os consumidores diretos e indiretos do mercado, afetando todo o funcionamento do sistema de saúde do país. O prejuízo das operadoras de saúde com fraudes impacta diretamente o valor das mensalidades pagas pelos beneficiários, uma vez que os custos envolvem o pagamento indevido da prestação de serviços de saúde. Outro fator que aumenta o custo do plano de saúde para o beneficiário é o uso inadequado dos serviços de saúde, como realizar consultas em excesso e desnecessárias, uso indevido de pronto-socorro e repetição de exames realizados recentemente, muitas vezes por desconhecimento do profissional de saúde acerca de seus resultados.

Fraude e golpes são duas formas de engano que podem causar prejuízos financeiros às suas vítimas e à sociedade. A fraude pode ser definida por um esquema ou ato ilícito cometido por meios enganosos para obtenção de ganhos pessoais, enquanto os golpes são projetados para manipular as vítimas para que forneçam suas informações voluntariamente.

Cometer atos fraudulentos contra o sistema de saúde é crime passível de punição com base na lei a todos os envolvidos, seja beneficiário de contrato pessoa física, familiar ou adesão. Nesses casos, o beneficiário que faz parte de um contrato empresarial, além da punição legal, também corre o risco de uma demissão por justa causa na empresa em que trabalha.

As fraudes contra a saúde suplementar ocorrem das mais variadas formas e, muitas vezes, com a participação do beneficiário, seja consciente da sua participação ou iludido em sua boa-fé. Para proteger e esclarecer seus beneficiários e a sociedade de modo geral sobre o uso adequado do plano de saúde, a Unimed Fesp elaborou as orientações disponibilizadas nesta cartilha.

O uso adequado do plano de saúde é uma responsabilidade de todos os beneficiários. Ele auxilia a prevenir as fraudes e evita desperdícios, ajudando no controle de custos e evitando reajustes mais altos das mensalidades.

Quando suspeitar de más práticas, faça sua denúncia para a Unimed Fesp por meio do nosso Canal de Denúncias. É anônimo e garantimos a confidencialidade.

Canal de Denúncias

<https://www.contatoseguro.com.br/unimedfesp>

Telefone: 0800 800 8989





DADOS PESSOAIS

DADOS PESSOAIS

1. Confira todas as suas informações na contratação do plano de saúde



O preenchimento da proposta de contratação do plano de saúde é de responsabilidade do beneficiário. Infelizmente, um dos maiores problemas identificados é a presença de informações divergentes e/ou omissão, como nome, idade, gênero, endereço, atividade profissional, vínculo empregatício ou associativo e condições de saúde, podendo configurar fraude, cancelamento e exclusão do beneficiário do plano de saúde. Além do risco de exclusão do plano após identificação da irregularidade, é passível de aplicação de sanções administrativas, cíveis e criminais.



O QUE FAZER

preencha você mesmo ou confira todos os dados informados no momento do preenchimento, antes da assinatura de sua proposta ou declaração de saúde. Isso irá garantir a cobertura adequada para os tratamentos e evitará maiores transtornos relacionados a penalidades aplicadas por fraude.

2. Informe os dados de saúde de forma correta

Além dos dados pessoais corretos no preenchimento do cadastro, os dados médicos do beneficiário devem ser preenchidos de forma adequada para que a operadora realize a análise da Declaração de Saúde. De acordo com as informações fornecidas, pode ser necessária a aplicação da Cobertura Parcial Temporária (CPT), restringindo algumas coberturas relacionadas à condição informada por até 24 meses.

Omitir informações sobre lesões e comorbidades e mentir sobre o peso e altura pode ser caracterizado como fraude, sujeitando o contrato a suspensão ou cancelamento, conforme regulamentação. O beneficiário que comete essa fraude está sujeito a sanções cíveis e criminais, além da possibilidade judicial de ressarcimento dos valores pagos indevidamente pela operadora, mediante a comprovação da omissão ou declaração falsa.



O que fazer:

preencher os dados corretos na declaração é responsabilidade do beneficiário, que pode ter apoio de um profissional médico de sua confiança para o preenchimento. No entanto, é preciso ter cuidado ao solicitar o preenchimento do documento por um terceiro, pois essa é sua responsabilidade enquanto beneficiário.



3. Carta de Permanência

A portabilidade de carências em planos de saúde é um direito dos beneficiários que possibilita a troca para outro plano, seja na mesma operadora ou em outra, sem a necessidade de cumprir novamente períodos de carência. A Carta de Permanência é o documento que possibilita essa migração e deve ser solicitado pelo beneficiário interessado na mudança. Esse documento contém dados pessoais do titular e dependentes e informações sobre o plano contratado na operadora de origem. Qualquer adulteração nos dados da Carta de Permanência configura fraude e pode ser classificada como estelionato. Quando identificada a fraude, o beneficiário tem o contrato cancelado e a operadora pode solicitar judicialmente a reparação de danos, além de outras sanções cíveis e criminais.



O que fazer

Confira se as informações na Carta de Permanência emitida pela sua operadora de origem estão corretas. Em caso de dúvidas, contate a operadora responsável pela emissão do documento ou a sua administradora de planos de saúde.



4. Mantenha seus dados atualizados na operadora

Também é de responsabilidade do beneficiário a atualização de seus dados cadastrais junto à operadora de saúde. Mantenha sempre suas informações atualizadas. Isso possibilitará que a operadora o contate sempre que necessário para informar mudanças e novidades do seu plano.



O que fazer

Informe diretamente o plano, ou sua corretora, associação ou empresa, sempre que houver alguma alteração relevante, como mudança de endereço e mudanças no contato telefônico e e-mail.



5. Não compartilhe a carteirinha e seu login e senha

A carteirinha do plano de saúde é um documento pessoal e intransferível. Emprestá-la ou permitir que outra pessoa se passe por você para usar seu plano de saúde é crime, e as pessoas envolvidas estão sujeitas às punições previstas em lei, como estelionato e falsidade ideológica.

Outra orientação importante é sobre o risco no compartilhamento do seu login e senha de acesso ao portal ou aplicativo da Unimed Fesp. Com esses dados, terceiros podem acessar informações pessoais e utilizá-las de forma inadequada, como alterar dados bancários, modificar valores ou solicitar reembolso de procedimentos não realizados.



O que fazer

- Nunca forneça sua carteirinha do plano a terceiros, seja ela física ou digital. Não compartilhe seu login e a senha de acesso ao aplicativo de beneficiário para evitar uso inadequado e ilegal das suas informações pessoais.
- Também não devem ser compartilhados os dados de acesso à plataforma gov.br, utilizada para solicitação de diversos



continua ▼



serviços governamentais, entre eles abertura de reclamações na Agência Nacional de Saúde Suplementar (ANS). Terceiros podem acessar suas informações, como dados da previdência social, declaração de imposto de renda, comprovante de vacinação e pendências fiscais. O uso indevido de dados alheios configura crime como estelionato, sujeito à multa e reclusão.

- A Unimed Fesp tem o compromisso de tratar dados pessoais, sejam de seus clientes, seus colaboradores e fornecedores, com o mais alto nível de cuidado, confidencialidade e conformidade com a Lei Geral de Proteção de Dados (LGPD) nº 13.709/2018.





**USO ADEQUADO DO
PLANO DE SAÚDE**

USO ADEQUADO DO PLANO DE SAÚDE

1. Verifique as informações contidas na sua guia de atendimento antes de assinar



Infelizmente, alguns prestadores incluem nas guias de atendimento alguns procedimentos que não foram realizados, e o fazem sem o conhecimento do beneficiário, aumentando os custos reais, e, conseqüentemente, o valor dos planos.

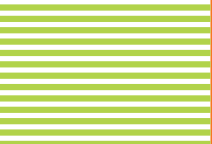
Entre as fraudes que podem ser cometidas pelo prestador de saúde em relação à guia de atendimento está a inclusão de exames durante a consulta médica; há também prestadores que atendem serviços de tratamentos seriados (como sessões de fisioterapia ou fonoaudiologia) que solicitam ao beneficiário a assinatura da guia informando todos os dias dos atendimentos, antes mesmo de serem realizados.



O que fazer

- Sempre que for atendido por um profissional ou prestador de serviços de saúde, verifique se todos os procedimentos realizados constam corretamente na guia de atendimento. O...

continua ▼



documento não pode estar em branco e deve ser assinado sempre após o procedimento ou consulta. Em caso de tratamentos seriados, assine a guia ao fim de cada dia de sessão.

- Evite deixar documentos e assinaturas salvas no prestador de serviço. Isso inibirá a utilização da sua assinatura em documentos em branco sem o seu consentimento.
 - Caso algum procedimento não tenha sido realizado, solicite a guia ao prestador para descarte do documento. Se ele se recusar a entregar, comunique a operadora de saúde sobre o ocorrido.
 - O aplicativo da Unimed Fesp oferece o recurso de token, uma forma prática e segura de liberar consultas, exames e tratamentos, com funcionamento semelhante ao token utilizado pelos bancos. Com apenas alguns toques no celular, você, beneficiário, autoriza seus atendimentos e adiciona uma camada importante de segurança, garantindo que apenas o próprio beneficiário possa validar os procedimentos. Isso reduz significativamente o risco de uso indevido do plano e de fraudes, problemas que impactam diretamente nos custos operacionais e podem influenciar nos valores das mensalidades e nos reajustes anuais.
- 

2. Exames desnecessários e repetitivos

A realização de exames e procedimentos desnecessários desperdiça recursos e pode representar riscos à saúde dos beneficiários, como a exposição à radiação e procedimentos invasivos, sendo que o principal motivo é a falta de acompanhamento contínuo por um profissional de saúde que tenha acesso ao histórico do beneficiário.



O que fazer

Informe sempre seu médico sobre exames realizados recentemente, assim como seu histórico médico, para que ele avalie a real necessidade de submetê-lo a novos procedimentos. Em cada nova consulta com seu médico ou médico de outra especialidade, leve os exames realizados mais recentes, mesmo que solicitados por médicos diferentes.



3. Use o pronto-socorro no caso de urgências emergências e use telemedicina em casos de baixa complexidade



O atendimento em pronto-socorro foca na resolução de problemas agudos da saúde, e o paciente apenas receberá os cuidados voltados para o sintoma apresentado naquele momento. Em sua grande maioria, os pacientes são medicados e dispensados para o acompanhamento da causa principal em consultório médico com agendamento. Além disso, muitas das situações de saúde que levam pacientes ao pronto-socorro não precisariam ser solucionadas em um hospital por tratar-se de problemas comuns, facilmente diagnosticáveis e tratáveis por um clínico geral, médico de família ou generalista. A ida desnecessária ao pronto-socorro pode expor o paciente a doenças e causar o agravamento de problemas de saúde. Ocasiona, também, o desperdício dos recursos de saúde utilizados em casos menos complexos (impactando no aumento dos preços dos planos de saúde), a menor personalização do cuidado e o aumento no tempo de espera na urgência, sendo que outro paciente com real necessidade poderia estar utilizando esse recurso.



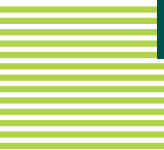
O que fazer

Procure sempre agendar a consulta eletiva, de preferência com um médico generalista, tratando assim a causa raiz dos problemas e não apenas os seus sintomas. Uma opção de consulta para casos de baixa complexidade é a telemedicina, cuja tecnologia é benéfica por ofertar uma assistência médica acessível, dispensando a necessidade de locomoção.





REEMBOLSOS



REEMBOLSOS

Reembolso é o ressarcimento das despesas assistenciais, como consultas, exames e outros procedimentos, realizadas pelo beneficiário junto a um prestador de serviço de sua escolha, de acordo com o estabelecido no contrato do plano de saúde do beneficiário com a operadora e conforme estabelecido pela ANS.

O reembolso só pode ser solicitado com a comprovação de que o serviço foi realizado e pago. Cabe ressaltar que a Unimed Fesp possui uma ampla rede credenciada de prestadores de serviços de saúde, prestadores qualificados e habilitados para oferecer um tratamento adequado aos beneficiários. No atendimento prestado pela rede credenciada não há necessidade de pagamento pelos serviços.

O reembolso solicitado fica registrado na sua DMED (Declaração de Serviços Médicos e de Saúde), um documento que profissionais e empresas de saúde enviam todo ano para a Receita Federal do Brasil. Essa declaração é uma forma do governo acompanhar as informações financeiras relacionadas a serviços de saúde e cruzar com as informações do imposto de renda dos beneficiários.

1. Falso facilitador ou Concierge

Alguns locais ofertam facilitador ou Concierge, sob a desculpa de agilizar a solicitação de seu reembolso. Solicitam seu login e senha de acesso ao aplicativo e portal do plano de saúde, tendo acesso a todos os seus dados pessoais. Sendo possível solicitar procedimentos não realizados e alterar dados bancários, tudo isso consentido pelo beneficiário para o cometimento de fraudes.



O que fazer

- Jamais compartilhe seus dados de login e senha com terceiros. É responsabilidade do beneficiário garantir a segurança dos seus dados, sendo que o compartilhamento com terceiros que pratiquem atos ilícitos é passível de crime previsto em lei. Se solicitarem esses dados a você, entre em contato imediatamente com a operadora e denuncie.
- Solicitar ou consultar o seu reembolso é simples e fácil por meio do seu aplicativo para celular ou portal da operadora, na Área do Cliente. Em caso de dúvida, sempre solicite ajuda da sua operadora de saúde.



2. Falsos procedimentos e documentos

O beneficiário deve estar atento à utilização de rede não credenciada, pois existem regras estabelecidas pela ANS, como a busca de rede pela operadora do plano de saúde e, caso não localizada, fornecer autorização para utilização de reembolso por meio de protocolo, podendo ser limitado a uma tabela de preço.

Contudo, os beneficiários acabam buscando procedimentos que não constam na cobertura do plano de saúde conforme o Rol de Procedimentos da ANS como, por exemplo, tratamentos estéticos. E, por conta disso, o procedimento é trocado por outro que seria coberto pelo Rol da ANS, sendo praticado um conluio entre beneficiário e prestador que emite recibos ou notas fiscais com descrição diferente do realizado, colocando em risco a saúde do próprio beneficiário.

Também podem ser considerados atos lesivos aumentar ou incrementar procedimentos ou alterar o valor para obter um reembolso maior. Esse tipo de fraude envolve tanto o beneficiário que solicita, quanto o prestador que altera o procedimento realizado para fins de obtenção de vantagem financeira.



O que fazer

- Após autorização do plano de saúde, anote o protocolo de atendimento e procure prestadores éticos que apresentem as notas fiscais e/ou recibos conforme o procedimento realizado.
- Antes de iniciar tratamentos com um prestador/médico não credenciado à operadora, procure a operadora de saúde e informe sua dificuldade de agendamento.



3. Fracionamento de recibo

Fracionamento de recibo ocorre quando uma única consulta ou procedimento é realizado, mas emite-se mais de um recibo ou nota fiscal, com o objetivo de conseguir um reembolso total de valor mais alto. Nesse caso, são considerados fraudadores tanto aqueles que recebem as notas fiscais ou recibos como aqueles que as emitem.



O que fazer

- O pedido de reembolso deve ser informado corretamente conforme o procedimento ou a consulta realizada e o valor efetivamente desembolsado, para pagamento com base nas cláusulas contratuais.



4. Reembolso sem desembolso ou reembolso assistido

Quando o beneficiário faz uma consulta ou procedimento em um prestador de serviço de saúde fora da rede credenciada sem a necessidade de pagamento direto ao prestador, ele pode estar sujeito ao golpe do reembolso sem desembolso ou reembolso assistido.

Nessa situação, o prestador de serviço apresenta um procedimento diferente e solicita os dados de acesso ao app e do plano de saúde, fazendo a solicitação de reembolso diretamente à operadora, aumentando o valor do atendimento para obter lucro ou incluindo procedimentos e exames não realizados. Esse é um tipo de fraude que pode não ser percebida pelo beneficiário, mas que pode envolvê-lo em um esquema fraudulento.



O que fazer

- Nunca informe seus dados em troca de oferta de ajuda para a solicitação de reembolso, e nem aceite atendimentos fora da rede credenciada da operadora sem a necessidade de pagamento prévio ao prestador. Faça você mesmo o pedido de reembolso diretamente à operadora e, em caso de dúvidas, consulte sua operadora de saúde.

Na Unimed Fesp, a solicitação de reembolso pode ser realizada via portal da operadora, na Área do Cliente, ou no aplicativo de celular.





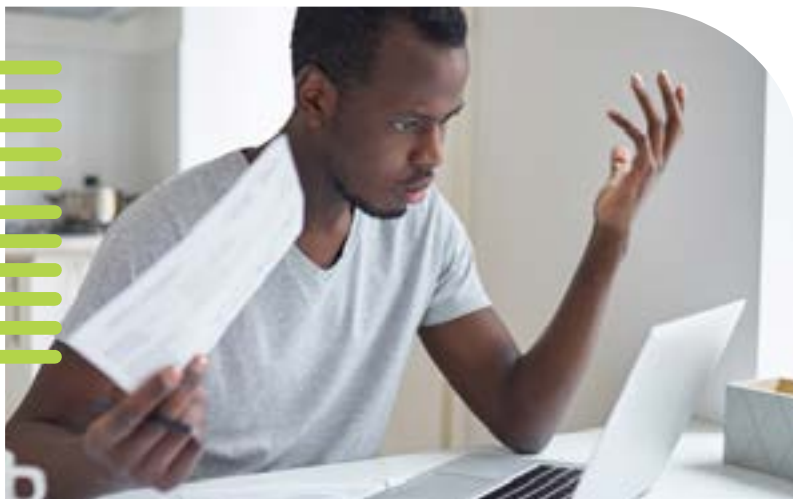
GOLPES

GOLPES

1. Atenção a falsos boletos

Crimes virtuais também afetam as operadoras de saúde e seus clientes. Os criminosos criam sites falsos ou outros recursos para emitir ou alterar boletos de planos de saúde, dando aparência de documento verdadeiro e enganando os beneficiários.

Nesses casos, o dinheiro depositado é desviado para a conta dos fraudadores, afetando diretamente os beneficiários.



O que fazer

Sempre que desconfiar de e-mails ou mensagens recebidas referente a cobranças, não faça o pagamento e consulte antes sua operadora de saúde.



CUIDADOS AO PAGAR UM BOLETO: PROTEJA-SE CONTRA FRAUDES

Ao efetuar o pagamento de um boleto, é crucial estar atento para evitar possíveis fraudes e golpes. Infelizmente, o cenário de boletos fraudados tem se tornado cada vez mais comum, colocando em risco a segurança financeira do beneficiário de plano de saúde. **Para protegê-lo, siga estas orientações:**

Verifique os dados do boleto

Antes de pagar qualquer boleto, confira atentamente os dados como nome do beneficiário, valor, vencimento, emissor e código de barras. Qualquer divergência pode ser indício de fraude:



Observe se o documento possui erros de português ou erros de digitação, fato comum em boletos falsificados.



Os últimos dígitos do código de barras correspondem ao valor a ser pago. É comum que os fraudadores não modifiquem esse campo.



O documento conter um valor diferente do que normalmente é pago pode ser um sinal de alerta.



Verifique se os primeiros dígitos do boleto coincidem com o código do banco emissor.



O valor do boleto aparece em dois lugares, no final do código de barras e no espaço “valor do documento”. Os valores precisam ser iguais.



CNPJ do emissor deve ser o mesmo da Unimed Fesp (43.643.139/0001-66).



Os números do código de barras devem ser exatamente iguais, tanto na parte superior quanto inferior do documento.



No campo “nome do pagador”, seus dados pessoais, como nome completo e CPF, devem estar corretos.



Segunda via de boleto

Caso seja necessário solicitar uma 2ª via do seu boleto, faça isso somente pelos canais oficiais da Unimed Fesp. Não busque por “segunda via de boleto Unimed Fesp” na Internet. Geralmente, ao fazer a busca nesse formato, você pode se deparar com uma página falsa que oferece o download da fatura falsa ou um link direcionado para uma conversa no WhatsApp, na qual você fornece seus dados e recebe uma fatura que parece ser verdadeira, mas não é. Evite clicar em links suspeitos enviados por e-mail ou mensagens.

Desconfie de descontos

Ofertas tentadoras com descontos podem ser iscas para golpes. Verifique a procedência do boleto e do vendedor antes de prosseguir com o pagamento.

Mantenha seu antivírus atualizado

Ter um antivírus atualizado em seu dispositivo pode ajudar a identificar e bloquear páginas falsas ou arquivos maliciosos que visam roubar informações.

Ao adotar essas medidas de precaução, você estará mais protegido contra possíveis fraudes relacionadas ao pagamento de boletos. Lembre-se sempre de manter a vigilância e a prudência ao lidar com transações financeiras pela internet.



2. PIX falso

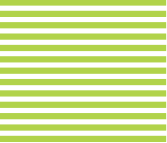
No golpe do pix falso, criminosos criam situações falsas, como pagamento via transferência para um CNPJ com um nome fantasia da Unimed Fesp em uma empresa de fachada. Ao receber o dinheiro, os golpistas desaparecem, deixando a vítima no prejuízo.



O que fazer

Verifique a legitimidade: antes de finalizar o pagamento, sempre confira se o CNPJ e o nome que aparece como beneficiário são os seus e da Unimed Fesp. Em caso de dúvida, não faça o pagamento e entre em contato com a Unimed Fesp pelos canais oficiais para verificar a autenticidade dos dados.

Caso tenha realizado o pix: o Banco Central tem uma ferramenta chamada Mecanismo Especial de Devolução (MED), criada para facilitar as devoluções em caso de fraudes, aumentando as possibilidades de a vítima reaver os recursos. Você deve registrar o pedido de devolução na sua instituição



bancária em até 80 dias da data em que você fez o pix, quando você for vítima de fraude, golpe ou crime. O banco avalia o caso e, se entender que faz parte do MED, o recebedor do seu Pix terá os recursos bloqueados da conta. O caso é analisado em até 7 dias. Se concluírem que foi fraude, em até 96 horas você receberá o dinheiro de volta. Para mais informações, acesse <https://www.bcb.gov.br/meubc/faqs/p/o-que-fazer-em-caso-de-golpe-fraude-ou-um-crime>

Não compartilhe informações sensíveis: nunca compartilhe informações pessoais, bancárias ou códigos de segurança com desconhecidos. Fique atento a solicitações de dados bancários que parecem suspeitas.

Use canais oficiais: realize transações financeiras somente por meio dos canais oficiais da Unimed Fesp. E lembre-se: evite clicar em links ou fornecer informações em plataformas desconhecidas.

3. Falsa Central de Atendimento

Neste golpe, os criminosos entram em contato com o beneficiário fingindo ser funcionários da Unimed Fesp, com a intenção de roubar dados ou dinheiro. O contato pode ser feito por ligação, WhatsApp ou SMS. Durante o contato, pode ser solicitada uma transferência bancária sob a ameaça de cancelamento do plano de saúde caso o valor não seja pago. Também é comum a promessa de um grande reembolso, que só será liberado mediante o pagamento de uma pequena quantia.



O que fazer

- Verifique os canais oficiais de atendimento no seu cartão, aplicativo ou site da Unimed Fesp.
- Não realize depósitos para liberar reembolsos de procedimentos já pagos. Caso receba uma solicitação desse tipo, denuncie.
- Não clique em links recebidos por mensagens de celular.
- Não ligue para números fornecidos por mensagens de celular.



4. Golpe aplicado em familiares de paciente internado

É comum criminosos se passarem por médicos ou funcionários de hospitais na tentativa de conseguirem dinheiro de familiares que têm algum parente internado.



Segundo o Sindicato dos Hospitais, Clínicas e Laboratórios do Estado de São Paulo (SindHosp), golpistas têm adentrado o sistema informativo de estabelecimentos de saúde e emitido cobranças às famílias com pacientes internados sobre a necessidade de cirurgias ou compra de medicamentos. Com os dados dos pacientes em mãos, os criminosos ligam para o familiar afirmando que há custo em aberto para a realização de um procedimento que o convênio médico não cobre. Em seguida, pedem depósitos bancários para que ele seja realizado com urgência.



O que fazer

- Caso receba alguma ligação semelhante, atente-se ao número que realizou a chamada, se é o mesmo do hospital e anote-o. Anote também a conta bancária beneficiária do correntista falso. Imediatamente, entre em contato com a administração do hospital ou tesouraria para ter informações sobre possíveis cobranças. Não efetue qualquer pagamento antes de verificar a veracidade junto ao hospital. Além do hospital, também entre em contato com o plano de saúde para saber sobre o procedimento médico.
- Por este golpe ser considerado estelionato, faça um boletim de ocorrência para denunciar o crime. Procure a Delegacia de Polícia mais próxima de sua casa ou realize o registro pela Delegacia Eletrônica.
- Jamais repasse informações por internet ou telefone sem confirmar se está falando com um canal oficial.

5. Cuidado com cobranças falsas para entrega de exames

Criminosos estão aplicando novo golpe utilizando engenharia social. Eles entram em contato com pacientes de hospitais, clínicas e laboratórios, que passaram por atendimentos recentes, informando serem representantes dessas instituições de saúde.

Dizem que o resultado de um exame realizado pelo paciente está disponível, porém, por motivo de falha no sistema, oferecem entrega domiciliar, mediante pagamento de uma pequena taxa. No momento da entrega, informam que o pagamento deve ser realizado somente por máquina de cartão para crédito ou débito. Os golpistas apresentam um equipamento com a tela quebrada ou adulterado para exibir o valor correto da taxa, mas realizam cobranças muito maiores na conta da vítima.





O que fazer

- Usualmente, as instituições de saúde acordam e cobram pela entrega domiciliar de resultados no dia da realização do exame. Em caso de contatos telefônicos ou mensagens posteriores que solicitem pagamentos para a entrega de resultados de exames ou outros serviços não previamente agendados, desconfie.
- Entre em contato diretamente ou, se possível, vá direto à instituição de saúde para verificar a veracidade da solicitação antes de efetuar o pagamento.
- Sempre evite fornecer dados pessoais ou financeiros por telefone ou aplicativos de mensagens.

Ao realizar pagamentos com cartão, siga estas orientações de segurança:

1. Nunca entregue seu cartão nas mãos do entregador ou de terceiros.
 2. Sempre confira o valor exibido na maquininha antes de digitar a senha ou aproximar o cartão. Se houver divergência, não conclua o pagamento e desconfie da situação.
 3. Após o pagamento, verifique o comprovante emitido e, se possível, consulte o extrato do cartão ou do banco para confirmar a transação.
 4. Em caso de qualquer suspeita, evite realizar o pagamento e busque alternativas seguras junto ao prestador do serviço.
 5. Ative as notificações do aplicativo do banco no celular.
- Caso suspeite de alguma tentativa de golpe, denuncie imediatamente às autoridades policiais.
 - Caso tenha sido vítima de um golpe, acione seu banco para bloqueio do cartão e registre um boletim de ocorrência.

6. Uso indevido da marca Unimed para aplicação de golpes



Por meio do uso indevido da marca Unimed, criminosos criam sites, perfis nas redes sociais, contas, e-mails, grupos, canais em aplicativos como WhatsApp/Telegram/WeChat entre outros, com objetivo de enganar e causar prejuízo ao consumidor através de ofertas, descontos inexistentes, vendas fraudulentas e boletos com dados bancários adulterados.

Além disso, é comum que falsos perfis de pessoas se passando por corretores simulem a venda de plano de saúde on-line, o consumidor faz o primeiro pagamento e não recebe a carteirinha. Ao entrar em contato com a operadora de saúde para cobrar o envio da carteirinha, o consumidor descobre que a venda nunca ocorreu e foi vítima de um golpe.

Golpistas, também, criam falsos anúncios em redes sociais com valores atrativos ou desconto no valor da mensalidade do plano de saúde. A publicação direciona o usuário para uma conversa via WhatsApp/Telegram/WeChat, ou outros meios de mensagens instantâneas, com um suposto colaborador da Unimed. Durante a conversa, os criminosos utilizam técnicas de engenharia social e/ou clickbait (isca digital), explorando

a confiança do consumidor, a urgência da oferta e a aparência de legitimidade da marca para induzir o compartilhamento de dados pessoais, envio de documentos, realização de pagamentos ou acesso a links e arquivos. Em alguns casos, o golpista pode solicitar a instalação de aplicativos ou o clique em links maliciosos; em outros, o prejuízo ocorre exclusivamente pelo fornecimento de informações sensíveis ou pela realização de transações financeiras indevidas. Essas práticas podem resultar no vazamento de dados pessoais, uso indevido de informações do beneficiário e acesso fraudulento a recursos financeiros.



O que fazer

- Verifique o site oficial da Unimed Fesp por meio dos canais de atendimento ou do aplicativo.
- Antes de contratar um plano de saúde, confirme com a Unimed Fesp se o corretor é credenciado.
- Não compartilhe informações pessoais ou sensíveis, como documentos, endereço, dados bancários, número de cartão ou informações de saúde, pela internet ou por aplicativos de mensagens.
- Não instale nenhum aplicativo que tenha sido solicitado por terceiros. O aplicativo oficial da Unimed Fesp chama-se Unimed SP – Clientes e está disponível na sua loja de aplicativos.
- Desconfie de ofertas com preços muito abaixo do mercado, promessas de vantagens imediatas ou solicitações de pagamentos de urgência.
- Não clique em links recebidos por e-mail, SMS ou aplicativos de mensagens.
- Só realize transações financeiras após certificar-se da autenticidade do emissor da cobrança e, na dúvida, entre em contato direto com os canais oficiais de atendimento da Unimed Fesp.

7. Falsas vagas de trabalho

O golpe das vagas de trabalho falsas ocorre quando criminosos criam anúncios de empregos atrativos em sites, redes sociais ou até mesmo via e-mail, se passando por empresas legítimas e oferecendo bons salários e benefícios. O objetivo desses golpes é obter dados pessoais e financeiros dos interessados ou até mesmo o pagamento de taxas para participação nos processos seletivos.



O que fazer

- Entre em contato diretamente com a Unimed Fesp, por meio dos canais oficiais, para confirmar a veracidade das vagas anunciadas.
- Desconfie de pagamento para qualquer fim ao participar de processos seletivos.
- Confirme a legitimidade da vaga antes de compartilhar dados pessoais.
- Não clique em links suspeitos ou forneça informações pessoais em páginas que não possuam certificado de segurança (<https://>).
- Desconfie de ofertas de trabalho com salários e benefícios muito acima da média de mercado ou que não exigem experiências ou habilidades específicas.
- Vaga muito genérica pode ser apenas uma isca para uma empresa que quer montar um banco de dados e vender serviços a potenciais clientes.
- Atenção com comunicação confusa e erros de digitação. Geralmente, empresas sérias fazem contatos bem redigidos e com uma comunicação clara e profissional.
- Quando receber um contato logo após terminar uma candidatura, é possível que alguém tenha acessado os seus dados preenchidos para a vaga e feito contato para oferecer algum produto ou serviço. Cuidado, é possivelmente uma fraude. Se isso acontecer, não assine, não compre nada e não compartilhe dados bancários.
- As vagas de trabalho da Unimed Fesp são divulgadas apenas pelos canais oficiais.

Foi vítima de um golpe? Veja o que você pode fazer

1. Em primeiro lugar, faça o registro de um Boletim de Ocorrência* na Polícia Civil do seu estado, seja em uma delegacia ou on-line.
2. Mantenha todas as informações relacionadas ao golpe guardadas para futuras investigações e processos judiciais. Registre datas, horários, nomes, números de telefone e quaisquer outras informações relevantes.

*Você sabe a diferença entre boletim de ocorrência e denúncia? A diferença é que o BO é um relatório oficial de um incidente, enquanto a denúncia é um ato legal que acusa alguém de atividade criminosa e inicia o processo judicial. O boletim de ocorrência é o primeiro passo para a coleta de informações em casos que podem se tornar uma denúncia e, posteriormente, um processo criminal.



Outras dicas importantes



Nunca deixe senhas e informações pré-cadastradas no aparelho celular.



Cuidado ao clicar em anúncios publicitários. Alguns podem conter links maliciosos.



Atenção ao participar dos jogos de perguntas e respostas em redes sociais. Alguns deles solicitam permissão para utilizar sua foto em simulações, na intenção de capturar suas informações pessoais e acessar seu dispositivo. Ao interagir com esse tipo de conteúdo, você pode autorizar a instalação de códigos maliciosos em seu telefone ou computador.

CONTATOS

CONTATOS



Central de Acolhimento e Experiência do Cliente (Caec)

0800-772-3030



Comercial

comercial@unimedfesp.coop.br – (11) 2146-2646 / (11) 4567-5413



Central de Autorizações

(11) 3385-6074



Ouvidoria

<https://www.unimed.coop.br/site/web/unimedfesp/ouvidoria>

SERVIÇOS AOS CLIENTES



Área do cliente

<https://portalclientes.unimedfesp.coop.br/>



Aplicativo Unimed SP Clientes

Disponível no Google Play e App Store

REFERÊNCIAS

- Cartilha de Prevenção e Combate a Golpes e Fraudes – Unimed do Brasil
- Cartilha de Prevenção e Combate às Fraudes – Seguros Unimed
- Cartilha de Prevenção Contra Golpes – Polícia Civil de Santa Catarina
- Cartilha Saúde sem Fraude – Federação Nacional de Saúde Suplementar (FenaSaúde)
- Estudo sobre Fraudes e Desperdícios em Saúde Suplementar. Novembro/2023 – Instituto de Estudos de Saúde Suplementar (IESS) e Ernst & Young
- Mecanismo Especial de Devolução (MED) de Pix, do Banco Central, disponível em <https://www.bcb.gov.br/meubc/faqs/p/o-que-e-e-como-funciona-o-mecanismo-especial-de-devolucao-med>
- Rever processos é importante para assegurar a proteção dos dados. Artigo publicado por SindHosp em 12/04/2022. Disponível em <https://sindhosp.org.br/protacao-dados-saude-golpe/>



USO CONSCIENTE DO PLANO DE SAÚDE

Dicas de prevenção à fraude e utilização
adequado dos serviços de saúde



<https://unimed.me/970/prevencaoafraude>



Unimed 
Fesp

ANS Nº 319996

Atualizado em maio de 2026.

