

1	Introdução	3
2	Dicas gerais de segurança para se prevenir	4
3	Golpes atuais mais comuns	5
	3.1 Abordagem de falso advogado	5
	3.2 Que envolvem o INSS	6
4	Providências em caso de ser vítima de golpe	14

1 Introdução

Golpes com temas jurídicos ou previdenciários tem se tornado cada vez mais frequentes e não tem sido diferente contra os médicos filiados ao Sinmed-MG, infelizmente. Nosso Departamento Jurídico tem se esforçado para denunciar os casos junto às autoridades competentes e dar apoio às vítimas, mas depois do infortúnio consumado, as dificuldades são grandes, de forma que a prevenção ainda é o melhor remédio. Nesse sentido, nossa equipe de assessores jurídicos desenvolveu esta cartilha com orientações sobre os golpes mais comuns relacionados a temas jurídicos e previdenciários. O objetivo é ajudar os médicos a identificar armadilhas e agir com prudência em situações que podem comprometer sua segurança financeira e jurídica.

Em situações suspeitas ou em caso de dúvidas o médico deve sempre entrar em contato com o Sinmed-MG através dos canais oficiais.

A prevenção é o melhor caminho. Conte conosco para esclarecer dúvidas e compartilhar este conhecimento com quem possa se beneficiar. Juntos, podemos combater fraudes e fortalecer a segurança contra estes golpes.

Boa leitura!

2 Dicas gerais de segurança

- **Ligue para o advogado** usando um número oficial ou conhecido;
- Não confie em mensagens de WhatsApp para tratar de assuntos financeiros;
- Compare os supostos documentos da Justiça com informações no processo judicial oficial (consultado diretamente no site do tribunal);
- Nunca transfira dinheiro antes de confirmar a autenticidade da solicitação;
- Configure a privacidade de seu WhatsApp para que apenas contatos conhecidos vejam sua foto de perfil;
- Utilize a função "Denunciar contato" para alertar a plataforma
 Whatsapp;
- Reúna todas as mensagens, documentos e informações relacionadas ao golpe e registre um boletim de ocorrência.

" Não confie em mensagens de WhatsApp para tratar assuntos financeiros"



3 Golpes atuais mais comuns

3.1 Golpe do falso advogado

Trata-se de golpe que configura o crime de estelionato previsto no art. 171 do Código Penal brasileiro

Vejamos abaixo como esse golpe é executado pelo estelionatário:

- Criminosos acessam o processo da pessoa na Justiça e coletam os dados;
- Em seguida, eles criam uma conta no WhatsApp com a foto e o nome do advogado da vítima;
- Depois, se passando pelo advogado, eles entram em contato com a vítima por mensagem e afirmam que ganharam a ação judicial;
- Para isso, eles falsificam documentos da Justiça para provar a veracidade da informação;
- No contato, eles alegam que é necessária fazer uma transferência bancária via pix para agilizar o recebimento da indenização;
- Após a transferência, os bandidos apagam todas as mensagens e bloqueiam o contato da vítima.

3.2 Golpes em temas previdenciários

 Fique atento às notificações de alteração de senhas enviadas aos seu e-mail ou whatsapp sobre o aplicativo meuinss.gov.br

Através do acesso a esse aplicativo os golpistas podem acessar a todos os seus dados e trocar o local (banco) de pagamento dos benefícios, fazer empréstimos, e muito mais. É importante que você aumente o nível de segurança da sua conta.

Caso esteja com alguma dificuldade para aumentar o nível da conta gov.br, esclareça suas dúvidas em:

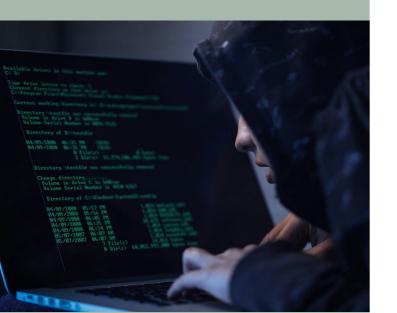
https://www.gov.br/governodigital/pt-br/acessibilidade-e-usuario/atendimento-gov.br/duvidas-no-aplicativo-gov.br/duvidas-gerais-no-aplicativo-gov.br

 Golpistas enviam mensagens falsas por e-mail, SMS ou redes sociais, que se parecem com comunicações legítimas de autoridades ou empresas confiáveis. Essas mensagens geralmente contêm links de páginas falsas com o intuito de fraude para obter ilegalmente informações pessoais como números de identidade, senhas bancárias, número de cartão de crédito, entre outras.



"Fique atento as notificações de alteração de senhas enviadas aos seu e-mail ou whatsapp"

" Golpistas usam os dados vazados para contratar seguros em nome dos aposentados"



A "farra dos descontos"

O escândalo veio à tona depois de um número expressivo de aposentados e pensionistas do INSS apresentarem a mesma reclamação: descontos não autorizados começaram a ser feitos na folha de pagamento de seus benefícios.

Contratação de Seguros sem Conhecimento

Golpistas usam os dados vazados para contratar seguros em nome dos aposentados sem que eles saibam. Em muitos casos, os aposentados só descobrem o golpe quando recebem cobranças inesperadas.

Ofertas de Empréstimos Consignados

Antes mesmo dos advogados comunicarem a liberação de um benefício para o cliente, as instituições financeiras já começaram a ligar para oferecer seus serviços. Aposentados são constantemente abordados por ligações oferecendo empréstimos consignados, prometem condições atrativas e rápida liberação do dinheiro, mas frequentemente escondem taxas abusivas e cláusulas desfavoráveis, levando muitos aposentados a contrair dívidas desnecessárias e difíceis de quitar.

"Essa cobrança é feita por um falso boleto ou transferência devalores direto para uma conta" Atrasados a receber mediante taxa - Mensagens de Whatsapp comunicando o pagamento de precatórios / RPV ou mesmo custas judiciais e pagamento de honorários

Os golpistas utilizam os dados vazados para personalizar a abordagem, tornando-a mais convincente. Incluem fotos com logomarca do escritório ou mesmo dos advogados, dados específicos do processo (o que é público) e até mesmo a logomarca dos tribunais. O golpe é antigo e pode ser praticado por telefone ou por e-mail. Um falso atendente do INSS ou da justiça faz contato com a vítima e lhe informa sobre valores de benefícios atrasados que foram liberados para o segurado, com atualização e correção de juros. Surpreso e contente com o dinheiro extra que vai entrar, o aposentado informa os dados pessoais. Na segunda etapa, é cobrada uma taxa administrativa a ser depositada pelo beneficiado para liberar o pagamento direto na conta do aposentado. Essa cobrança é feita por um falso boleto ou transferência de valores direto para uma conta.

Roubo de Identidade

Com os dados vazados, criminosos podem cometer roubo de identidade, usando as informações para abrir contas bancárias, solicitar cartões de crédito ou realizar outras transações fraudulentas.

Acesso a senhas do Portal GOV.BR

Os golpistas entram no portal utilizando senhas e realizam empréstimos, alteram o banco de recebimento do pagamento, entre outras.

Golpe da prova de vida

Pessoas mal-intencionadas se passam por servidores do INSS e visitam ou telefonam para os beneficiários em casa para, supostamente, fazer a comprovação de vida e, assim, coletar dados e praticar delitos.

Prova de vida online

Os criminosos ligam para aposentados e pensionistas alertando sobre a necessidade de realizar uma prova de vida digital, modalidade nova. Para a operação, o falso atendente do INSS pede para a vítima confirmar os dados pessoais e bancários.

"Criminosos podem cometer roubo de identidade, para abrir contas bancárias, solicitar cartões de crédito ou realizar outras transações fraudulentas"



Benefício bloqueado

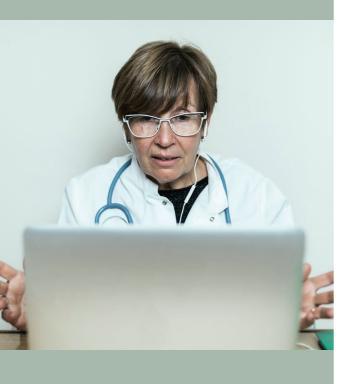
O aposentado recebe a ligação de um falso atendente do INSS alertando para o bloqueio iminente do benefício por desatualização de dados cadastrais. O falso atendente argumenta que para atualizar é fácil, basta que o aposentado lhe forneça informações como CPF, endereço, data de nascimento, dados bancários, número do cartão do INSS e outras informações. Convencido de que está conversando com um servidor do INSS, o aposentado fornece as informações solicitadas. Os dados são suficientes para o criminoso cometer fraudes em nome do segurado.

Agendamento de perícia médica

A perícia médica deve ser feita periodicamente por segurados de benefícios por incapacidade temporária ou continuada. Os criminosos fazem contato com as vítimas para agendar a consulta. Solicitam informações do beneficiado como endereço, RG, CPF, dados bancários e até senhas em algumas situações. Depois solicitam envio de foto atual e documentos digitalizados. Com os dados, foto e documentos, os criminosos podem realizar fraudes financeiras.

O INSS alerta para que o segurado não forneça os dados. O instituto apenas pede informações ou documentos pelo sistema Meu INSS. As convocações poderão chegar por carta, notificação do banco pagador, e-mail ou publicação no Diário Oficial da União e sempre estarão registradas no perfil do segurado no site Meu INSS com prazo e orientações para agendamento.





Antecipação do 13° salário e consignado

Via de regra, o 13° salário é antecipado em parte para os aposentados do INSS para recebimento em junho. Os criminosos, cientes desse calendário, fazem contato com o segurado para oferecer um adiantamento dos valores mediante uma taxa. O falso atendente de uma financeira solicita dados e cópia dos documentos para autorizar a operação. O aposentado que recebe a oferta paga a taxa e envia as informações, porém não recebe o dinheiro. Muitas vezes ainda pode ser vítima do falso empréstimo consignado, em que os criminosos operam como agentes de financeiras e autorizam o crédito em nome da vítima. O dinheiro cai na conta do segurado, porém as parcelas com juros também. Para o golpista, a vantagem é ficar com as comissões que remuneram o agente de crédito e a instituição responsável por intermediar o empréstimo.

Golpes com Falsos Benefícios

Golpistas prometem benefícios adicionais ou aumentos na aposentadoria em troca de um pagamento antecipado. Utilizando táticas persuasivas, eles convencem os aposentados a fazer transferências de dinheiro, prometendo vantagens que nunca se concretizam. As vítimas não só perdem dinheiro, mas também a confiança em instituições legítimas que oferecem benefícios reais.

Como os golpistas conseguem as informações dos beneficiários?

Segundo o INSS, foram identificadas brechas de acesso aos sistemas do órgão. Basicamente, ex-funcionários do Instituto — ou até mesmo aqueles que já faleceram — continuavam com usuários ativos no sistema.

Logo, os acessos pessoais (usuário e senha) dessas pessoas podem ter sido utilizados para adentrar o sistema do INSS e coletar informações sensíveis de milhares de segurados.

" Foram identificadas brechas de acesso aos sistemas do órgão "



Como ajudar os aposentados a se protegerem?

- É essencial não compartilhar informações pessoais ou bancárias por telefone ou internet ou por pessoas que se dizem servidores do INSS que solicitam informações sobre prova de vida ou outras informações;
- Entre em contato diretamente com o seu advogado através dos canais oficiais;
- Siga o Instagram oficial do INSS = inss_oficial_gov;
- Em casos de ligações suspeitas, é preciso evitar o fornecimento de informações pessoais e denunciar imediatamente
- Entidades como o Procon e a Polícia Federal oferecem suporte e orientações para evitar fraudes;
- Ofertas de empréstimos ou seguros que parecem vantajosas demais precisam ser encaradas com desconfiança;
- Um bom hábito é **checar mensalmente os registros de pagamento do benefício**. Assim, é possível identificar mais rapidamente os descontos indevidos;
- Consulte sempre fontes confiáveis e busque ajuda ao menor sinal de golpe;
- Registre um Boletim de Ocorrência na Polícia Civil do seu estado ou DF. Detalhe a situação no registro e anexe cópias dos
 e-mails ou telas que comprovem a atividade indevida na conta gov.br. Toda e qualquer investigação será iniciada e realizada
 apenas pela polícia.

Denunciar tentativas de golpe é crucial, pois ajuda as autoridades a rastrear e punir os criminosos, além de alertar outros aposentados sobre os riscos.

4 Providências em caso de ser vítima de golpe

- Vítimas de golpes envolvendo o meio de pagamento eletrônico Pix devem, imediatamente, solicitar a devolução do valor ao banco.
 Para tanto, é necessário entrar em contato com o banco por telefone ou pelo aplicativo, relatar o ocorrido e pedir a devolução do dinheiro;
- Sempre anote o número de protocolo do atendimento;
- O Banco Central disponibiliza o Mecanismo Especial de Devolução (MED)¹, que foi criado para facilitar as devoluções em caso de fraudes, aumentando as chances de a vítima reaver as quantias transferidas.



" Imediatamente, solicitar a devolução do valor ao banco "

¹ Disponível em: https://www.bcb.gov.br/meubc/faqs/p/o-que-e-e-como-funciona-o-mecanismo-especial-de-devolucao-med.

- O prazo para registrar o pedido de devolução deve ser feito na instituição financeira em até 80 dias contados da data em que o Pix foi feito;
- Os golpes mencionados nesta cartilha configuram o crime de estelionato, que está previsto no art. 171 do Código Penal;
- O crime de estelionato somente se procede mediante representação da vítima, conforme previsto no § 5° do art. 171 do Código Penal. Ou seja, para que a autoridade policial possa investigar o golpista é necessário que a vítima faça uma representação contra o sujeito que praticou o estelionato;
- Para fazer a representação, a vítima pode comparecer à delegacia local e registrar um boletim de ocorrência solicitando que sejam tomadas providências contra os responsáveis pelo golpe;
- Também é possível a contratação de um advogado para redigir uma petição, juntando todos os documentos que comprovam o golpe, para representar

- perante o juiz ou Ministério Público, a fim iniciar as investigações ou até mesmo o processo criminal;
- O boletim de ocorrência deve ser feito também para relatar que os golpistas possuem seus dados pessoais, de modo que seja relatado no BO os dados obtidos pelos estelionatários;
- A vítima possui o prazo de seis meses para realizar a representação, de modo que este prazo começa a contar a partir do dia em que a vítima toma conhecimento do autor do golpe;
- É muito importante que a vítima faça a representação criminal, uma vez que é condição necessária para o início da investigação e, posteriormente, para possibilitar o oferecimento da denúncia contra o golpista. No curso da investigação podem ser produzidas provas que auxiliarão a vítima a recuperar os valores perdidos, bem como servirá de proteção para impedir que outras pessoas caiam no mesmo golpe.

PARCERIAS













Departamento Jurídico 31 99302.0106 | 31 3241.2811 www.sinmedmg.org.br @sinmedmg