A iugu adota as melhores práticas do mercado e segue padrões e frameworks internacionais para garantir sua segurança. É importante que você saiba que a iugu não realiza as seguintes ações:

- » Não solicita depósito em contas bancárias de terceiros.
- » Não solicita atualização de seus dados cadastrais por e-mail, sms ou telefone. (exceto se houver um ticket aberto pelo cliente).
- » Não solicita instalação de programas, exceto para atualizações de segurança para acesso às aplicações da iugu.
- » Não solicita senha, códigos de segurança de suas contas via e-mail ou telefone, exceto o ID da conta do cliente durante o atendimento.
- » Não solicita informações como senha, código de token, número e/ou foto do seu cartão, CVV (código de verificação do cartão), entre outros dados em e-mails.

PROTEGENDO SUAS SENHAS E DISPOSITIVOS

- Sempre use código de bloqueio ou senha para acessar seu aparelho celular ou computador, e habilite o bloqueio automático de ambos para o menor tempo possível.
- Nunca anote suas senhas, armazene-as em arquivos comuns e sem proteção no seu computador.
- Caso tenha necessidade de administrar grande quantidade de credenciais e contas, utilize algum gerenciador de senhas.
- Crie senhas que contenham no mínimo 8 caracteres (senhas longas são mais seguras, logo o recomendado é de 12 caracteres ou mais se possível), utilizando ao menos duas combinações: letra maiúscula, letra minúscula, número ou caractere especial e não utilize sequências numéricas ou do teclado. Por exemplo: M1nh@$enh@ehF0rte3.
- Utilize ferramentas de segurança como biometria e dupla (2FA) ou múltipla autenticação (MFA) em seus aplicativos e e-mail.
- Nunca deixe o seu token exposto em repositórios de compartilhamento e de colaboração de códigos (por exemplo: GitHub).
- Se precisar armazenar o seu token, guarde-o em um cofre de senhas, um local seguro e privado para evitar vazamento de informações.
- Nunca utilize o recurso de “lembrar/salvar senha” em navegadores e sites de internet.
- Nunca compartilhe suas credenciais e senhas com outras pessoas, estas são suas identidades no mundo digital.
- Altere sua senha com frequência e utilize uma senha diferente para cada serviço/site da internet.
- Evite fazer transações financeiras em sites de comércio eletrônico, bancos e na iugu utilizando redes Wi-Fi públicas (ex.: cyber cafés, aeroportos e hotéis).
- Tenha sempre uma solução de antivírus instalada e atualizada em seu dispositivo eletrônico.

A iugu não tem responsabilidade por danos causados em decorrência de serviços disponibilizados por terceiros ou pela segurança de terceiros e não terceiriza seu website e ou plataforma, a iugu apenas atua como uma intermediadora de pagamento.

PREVENINDO FRAUDES

- Não pague boletos de fontes desconhecidas, se você desconfia da autenticidade de um boleto, não pague e entre em contato conosco através do canal Ajuda e Suporte em nosso site.
- Antes de fornecer dados de pagamento, certifique-se de que o endereço apresentado em seu browser corresponde ao site da iugu.
- O site da iugu sempre faz uso de conexão segura, ou seja, os dados transmitidos entre seu navegador e o site serão criptografados.
- Fique atento (a) no seu extrato e nas confirmações das transações. Caso identifique uma transação estranha, entre em contato através do canal Ajuda e Suporte em nosso site.
- Caso seja vítima de um golpe, entre em contato imediatamente com a sua instituição financeira e acione a polícia.
- Redefina suas senhas ou solicite o bloqueio da conta.
- Faça um boletim de ocorrência, pois este servirá como comprovação do fato posteriormente.
- Caso tenha recebido algum e-mail, SMS ou ligação suspeita, ou se acredita ter sido vítima de uma fraude envolvendo a iugu, entre em contato através do canal Ajuda e Suporte em nosso site.

SMS E CONTATO TELEFÔNICO FALSOS:

- Utilize somente os canais oficiais informados no Site para assuntos relacionados à sua conta, cartão ou atualização de dados cadastrais.
- Jamais forneça (verbalmente ou digitando) dados pessoais, senhas, códigos de identificação do aparelho celular (IMEI), números de cartão de crédito, CVV ou outras informações bancárias por contato telefônico ou com ninguém. A iugu não solicita atualização cadastral por este meio.
- Ao desligar, antes de qualquer ação sugerida no contato telefônico, acione nosso canal Ajuda e Suporte em nosso site utilizando um outro aparelho celular.

GOLPES USANDO O PIX:

- Sempre faça o cadastramento do Pix nos aplicativos e canais oficiais da iugu.
- Desconfie de e-mails ou SMS com ofertas de dinheiro fácil ou prêmios em troca do cadastramento do Pix. Evite acessar links sobre o cadastramento do Pix recebidos por SMS e e-mails.
- A iugu não acessa os dispositivos de seus clientes remotamente para habilitação do Pix. Nunca aceite ofertas de manutenções (presencial ou remotamente) em seu computador ou aparelho celular para a utilização do Pix.
- A iugu não entra em contato oferecendo ajuda para cadastramento de chave Pix e nem solicita informações como senha, código de token, número e/ou foto do seu cartão, CVV, entre outros dados em contatos telefônicos.

INVASÃO DE CONTA:

- Não clique em links suspeitos, fique atento às mensagens ou links que peçam sincronização, atualização de senhas, chaves de acesso ou novos cadastros. Na dúvida entre em contato conosco através do canal Ajuda e Suporte em nosso site.
- Não responda mensagens suspeitas e sempre verifique o número de quem está enviando. Em caso se suspeita de alguma conta comprometida, troque imediatamente suas senhas.

GOLPE DO BOLETO FALSO:

- Independentemente do canal utilizado para pagamento (caixa eletrônico, mobile banking, internet banking, etc.) serão mostrados os dados do beneficiário (a empresa ou pessoa que receberá o dinheiro). Se na informação que aparecer na tela, a conta em questão não pertencer ao beneficiário correto, o cliente não deve concluir a operação. Confirme seus dados pessoais, como CPF, e busque por erros gramaticais e de formatação. Suspeite se uma cobrança recorrente vier com variação de valor inesperada.

CONHEÇA OS CANAIS OFICIAIS DA IUGU

Você pode encontrar a gente nos seguintes canais oficiais: Instagram, Facebook, LinkedIn, Twitter, Youtube e Site.

A iugu não possui outras comunidades ou grupos além dos citados acima, desconfie de outros perfis, mesmo que eles se identifiquem como “não oficiais”. Nosso único canal de suporte aos clientes é através do canal Ajuda e Suporte em nosso site.

Tome cuidado se alguém se identificar como colaborador da iugu em qualquer grupo ou rede social, pois pode ser uma pessoa tentando obter suas informações para realizar fraudes. Nenhum colaborador da iugu está autorizado a oferecer ajuda ou pedir informações via redes sociais ou aplicativos de comunicação (como Whatsapp Telegram).

Conheça também nossa Política de Segurança da Informação e nossa Política de Privacidade

Sejam Bem-vindos (as) à iugu!