

Segurança de Transações e Conta

A segurança da conta é importante para nós e tomamos várias medidas para proteger as informações relacionadas à sua conta Remitly. Você também pode fazer certas coisas que ajudarão a proteger sua conta e suas informações pessoais.

Processos de Verificação de Conta

Sua conta Remitly está sujeita a procedimentos de verificação para manter altos níveis de segurança, confiança e proteção.

Se você é um novo cliente Remitly e criou uma nova conta Remitly usando o site da Remitly, você deve fornecer certas informações pessoais e concluir o processo de verificação por e-mail.

Depois que sua conta estiver ativa, implantamos uma variedade de procedimentos manuais e automatizados de gerenciamento de risco que nos permitem identificar atividades suspeitas na conta. O objetivo é identificar quaisquer características que pareçam incomuns ou inconsistentes com seu uso anterior. Como parte desse processo, contratamos prestadores de serviços líderes do setor para verificar informações pessoais e financeiras. Esses serviços nunca entrarão em contato com você diretamente nem usarão suas informações para nada além da conclusão bem-sucedida da transação pretendida.

Segurança de Senha

Quando você faz login na sua conta, tomamos certas medidas para protegê-la. Primeiro, sempre que você faz login na sua conta Remitly, você se conecta usando uma conexão de servidor segura (<https://>). Usamos Secure Socket Layer (SSL) com criptografia de 256 bits, o padrão do setor em proteção de servidor seguro.

Sua conta também é protegida por uma senha exclusiva que você cria. Você não deve usar palavras ou frases comuns como senha. Em vez disso, sua senha deve ter pelo menos oito caracteres, incluindo números e letras em maiúsculas e minúsculas. Você deve manter essa senha em sigilo. Compartilhar sua senha reduzirá a segurança da sua conta Remitly.

Cuidado com Golpes na Internet

- NÃO faça um pagamento para reivindicar prêmios de loteria ou concursos, nem com base em promessas de receber uma grande quantia em dinheiro.
- NÃO faça um pagamento porque lhe "garantiram" um cartão de crédito ou

empréstimo.

- NÃO responda a uma oferta na Internet ou por telefone que você não tenha certeza de ser legítima.
- NÃO faça um pagamento para alguém que você não conhece ou cuja identidade não pode verificar.

Em caso de dúvida, peça ao destinatário mais informações sobre a finalidade e a segurança do pagamento solicitado. Não envie o pagamento até que você se sinta confortável com a transação.

Identificando E-mails de Phishing ou Falsificados

Em algum momento, você pode receber um e-mail que parece ter sido enviado pela Remitly, mas que na verdade não é genuíno. Esse e-mail pode direcioná-lo a um site com aparência semelhante ao site da Remitly. Você pode até ser solicitado a fornecer informações da conta, como seu endereço de e-mail e senha.

Esses sites falsos podem roubar suas informações confidenciais de conta e pagamento para cometer fraudes. Esses e-mails falsos podem conter vírus ou malware que detectam senhas ou dados confidenciais. Por isso, recomendamos que você instale um programa antivírus e o mantenha sempre atualizado.

Aqui estão alguns pontos importantes a ter em mente como parte de uma defesa contra e-mails fraudulentos:

- Seu número completo de CPF ou data de nascimento
- O número do seu cartão de crédito, PIN ou código de segurança do cartão de crédito (incluindo "atualizações" de qualquer um dos itens acima)

Recomendamos que você não abra nenhum anexo de e-mail de fontes suspeitas ou desconhecidas. Anexos de e-mail podem conter vírus que infectam seu computador quando o anexo é aberto. Se você receber um e-mail suspeito supostamente enviado pela Remitly que contenha um anexo, recomendamos que você exclua o e-mail sem abrir o anexo.

Fique atento a erros gramaticais ou tipográficos. Alguns e-mails de phishing são traduzidos de outros idiomas ou enviados sem revisão e, como resultado, contêm erros gramaticais ou tipográficos.

O e-mail é da Remitly? Embora os phishers possam enviar um e-mail falsificado para que pareça ter sido enviado pela Remitly, às vezes você pode determinar se é autêntico verificando o endereço de retorno. Se a linha "de" do e-mail parecer "remitly-security@hotmail.com" ou "remitly-fraud@msn.com", ou contiver o nome de outro

provedor de serviços de Internet, pode ter certeza de que não é genuíno.

Os sites genuínos da Remitly estão sempre hospedados no seguinte domínio: https://www.remitly.com/

Às vezes, o link incluído em e-mails falsificados parece um endereço genuíno da Remitly. Você pode verificar para onde ele realmente aponta passando o mouse sobre o link; o site real para onde ele aponta será exibido na barra de status na parte inferior da janela do navegador ou como um pop-up.

Nunca usamos um endereço web hospedado em um domínio diferente dos listados acima. Por exemplo, domínios variantes como "https://security-payments-remitly.com/. . ." ou um endereço IP (sequência de números) seguido de diretórios como "https://123.456.789.123/remitly.com/. . ." não são sites válidos da Remitly.

Além disso, às vezes o e-mail falsificado é configurado de modo que, se você clicar em qualquer lugar no texto, será direcionado ao site fraudulento. A Remitly nunca enviará um e-mail que faça isso. Se você clicar acidentalmente em tal e-mail e for para um site falsificado, não insira nenhuma informação; em vez disso, apenas feche a janela do navegador.

Em caso de dúvida, não clique no link incluído em um e-mail. Acesse diretamente https://www.remitly.com/ e clique em **Minha Conta** no menu superior direito para visualizar compras recentes ou revisar as informações da sua conta. Se não conseguir acessar sua conta ou se observar qualquer coisa suspeita, avise-nos imediatamente.

Se você clicou em um e-mail falsificado ou suspeito e inseriu as informações da sua conta Remitly, você deve **imediatamente** atualizar sua senha. Você pode fazer isso acessando diretamente <https://www.remitly.com/> e clicando em **Configurações da Conta**. Na próxima página, clique em **Alterar suas informações pessoais, endereço de e-mail ou senha**.

Se você enviou o número do seu cartão de crédito ao site vinculado à mensagem de e-mail falsificada, aconselhamos que tome medidas para proteger suas informações. Você pode querer entrar em contato com a operadora do seu cartão de crédito, por exemplo, para notificá-la sobre o assunto. Por fim, você deve excluir esse cartão de crédito da sua conta Remitly para impedir que alguém obtenha acesso indevido à sua conta.

Se você recebeu um e-mail que sabe ser falso, ou se acredita ter sido vítima de um ataque de phishing e está preocupado com sua conta Remitly, avise-nos imediatamente reportando um [e-mail de phishing ou falsificado](/home/contact/).