



CUIDADO COM OS GOLPES

01 APRESENTAÇÃO

02 PRINCIPAIS GOLPES

Boleto Falso

Clonagem WhatsApp

Falsa troca de aparelho

Falsa visita técnica

Falsa conta digital

Instalação da Internet Fixa

Mensagem de texto com fraude em boleto

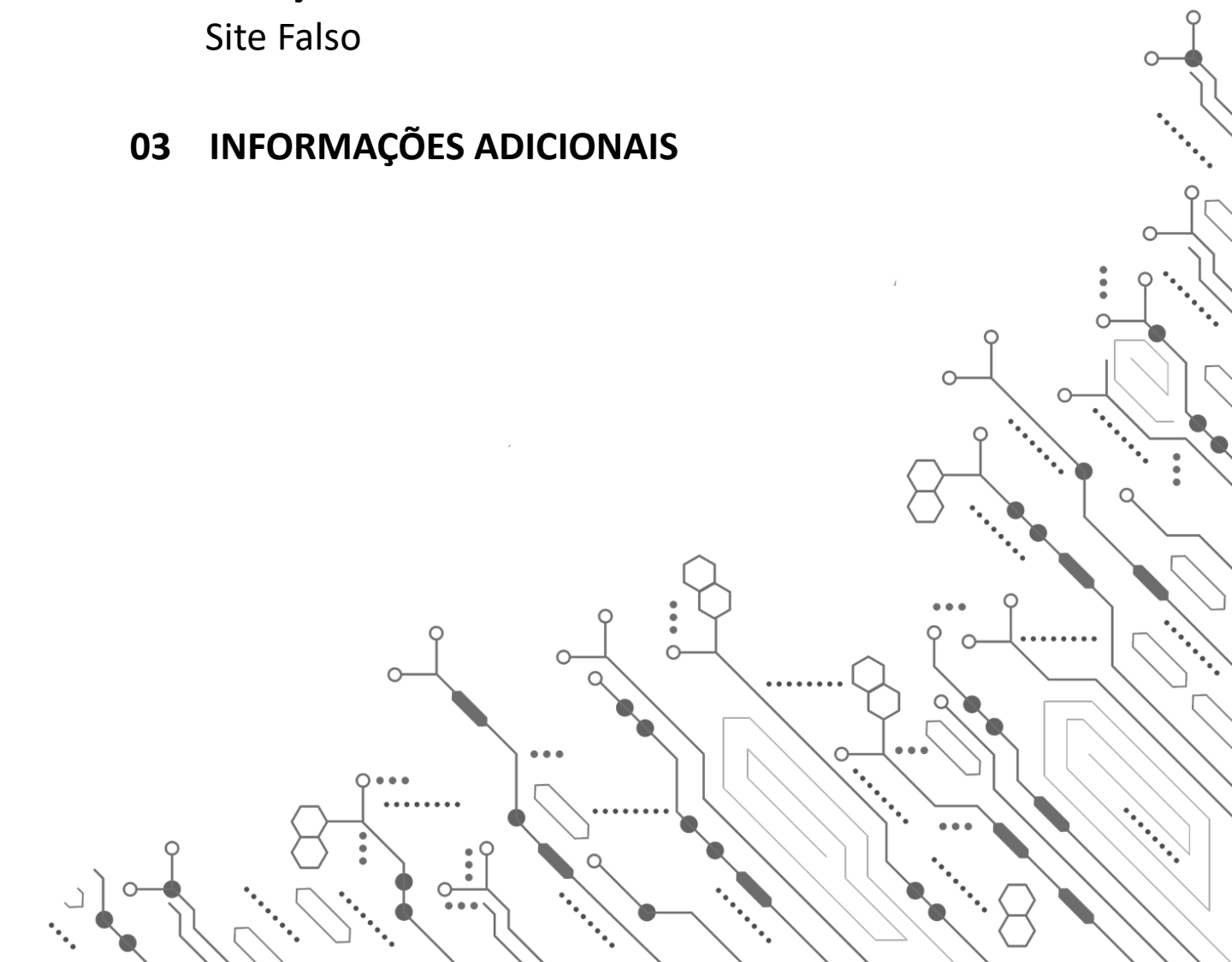
Mensagem de texto falsa

Obtenção do código Claro

Redução de Custos

Site Falso

03 INFORMAÇÕES ADICIONAIS



Este guia foi escrito com o objetivo de orientar você e sua família quanto aos golpes que estão sendo praticados na atualidade. Baseado em diversos materiais do mercado como cartilha de segurança para a internet, materiais divulgados pela Polícia e as melhores práticas de segurança.

Os criminosos estão sempre criando novas formas de ganhar dinheiro facilmente, tornando esse material obsoleto rapidamente, mas lembre-se que os golpes são cíclicos, ou seja, eles voltam a utilizá-los, mudando pequenos detalhes.

Esperamos que esse conteúdo possa auxiliar as pessoas evitarem a cair em golpes. Repassem os conhecimentos contidos aqui a seus familiares e amigos, para se prevenirem.



Lembre-se:

Segurança da Informação é responsabilidade de todos!

Boa leitura.



Como funciona?

As compras pela internet estão cada vez mais frequentes, agora nas redes sociais e até mesmo por WhatsApp. Muitas vezes a vítima não está com acesso seguro aos sites visitados, seja pelo computador, seja pelo celular.

Diversas são as formas de manipular a vítima neste momento. Pode ser por uma falsa página de alguma loja ou falso contato pelo WhatsApp para venda direta. Neste momento é emitido o boleto bancário para pagamento da compra efetuada. Este boleto possui cabeçalho e imagens aparentemente da loja/empresa em que a vítima estava negociando.

O golpe pode ser realizado tanto com a manipulação do código de barras do documento ou com a criação de páginas falsas que oferecem o download da “fatura”. Neste momento o valor transferido/pago vai para a conta bancária do golpista ou de um “laranja*”.

 **Dica:** Verifique sempre os dados do destinatário do boleto emitido. Antes de confirmar a transação ou pagamento, verifique se os dados do beneficiário conferem com os dados da loja/empresa.

Caso queira emitir uma 2ª via de algum boleto, procure o site oficial do credor e verifique os dados do boleto emitido.

Não pague boletos que recebeu através de e-mails que não estava esperando.

Confirme a veracidade deles no site oficial das empresas.

Evite fazer negociações com empresas que possuem avaliações negativas na internet, assim você protege o seu patrimônio.

*Laranja: é um termo utilizado para representar uma pessoa que intermedeia, voluntária ou involuntariamente, transações financeiras fraudulentas, emprestando seu nome, documentos ou conta bancária para ocultar a identidade de quem a contrata.



Como funciona?

Os golpistas têm diversos meios de conseguir o número da vítima, o mais comum é através de vazamento de informações de empresas. As vítimas recebem um SMS (mensagem) no qual consta um código de 6 dígitos. O golpista se passa por funcionário da plataforma de anúncio e/ ou outras empresas e solicita este código, alegando que isso é necessário para ativar o anúncio e/ ou efetivar uma compra.

Este código é uma verificação de segurança do WhatsApp, ou seja, o golpista digitou o número de celular da vítima no celular dele para ativar o WhatsApp. Este código de verificação para habilitar o WhatsApp foi enviado para o celular da vítima.

Informando o código você está desviando o seu número para o aplicativo instalado no aparelho do fraudador. Com tal feito, ele conversa com seus amigos, como se fosse você, pede dinheiro emprestado e faz outras vítimas. Assim que a transferência é feita, eles também se tornam vítima do golpe.



Dica: É muito importante habilitar a “confirmação em duas etapas” do WhatsApp. Para isso, clique em “Configurações/Ajustes”, depois clique em “Conta” e depois em “confirmação em duas etapas”; habilitar senha de 6 dígitos numéricos.

JAMAIS compartilhe o código de 6 números que chegar por SMS.

Caso tenha enviado o código e caído no golpe, envie um e-mail para support@whatsapp.com pedindo a desativação temporária de sua conta, explicando o ocorrido, bem como o seu número (exemplo: +55-11-9XXXX-XXXX); Após receber o e-mail do WhatsApp no prazo de 30 dias, configure-o com o seu número de celular.

Caso você receba uma mensagem de algum contato seu solicitando empréstimo de dinheiro ou depósito de algum valor, verifique com seu amigo a veracidade desta solicitação. E, caso seja verdade, antes de qualquer confirmação de depósito, verifique o destinatário (nome, CPF, agência bancária).



Como funciona?

O usuário recebe uma ligação, normalmente a cobrar de um número com bloqueio de identificação. Uma pessoa se apresenta como funcionário de uma operadora de telefonia celular com nome, matrícula e até um número de protocolo de atendimento. Essa pessoa oferece a troca do seu celular por um modelo mais novo, de tecnologia, a um preço convidativo. Diz que o usuário foi contemplado com a promoção da operadora e que, para receber o novo aparelho em casa pelos correios basta autorizar o pagamento do valor proporcional via cartão de crédito. Em alguns casos, se o usuário recusa a oferta, o golpista força a troca do aparelho, afirmando que é obrigatória.



Dica: A Claro esclarece que, embora entre em contato com seus clientes por celular, nunca liga a cobrar nem obriga seus clientes a realizar qualquer tipo de operação. Fique atento ao atender ligações de números não identificados no visor do seu celular e redobre sua atenção em ligações como essa. Em caso de dúvida, termine a ligação e informe-se diretamente com a Claro a respeito das promoções vigentes. Se isso já aconteceu com você, avise a polícia o mais rápido possível. No caso de ter informado seus dados bancários ou do cartão de crédito, contate seu banco ou administradora do cartão imediatamente solicitando as devidas providências.



Como funciona?

Uma pessoa se faz passar por técnico da Claro para reparos e instalações em sua residência. Muitas vezes devidamente uniformizado e com um crachá falso.



Dica: Nunca encaminhamos técnicos para sua casa sem termos falado com você antes.

Nossa visita técnica somente acontece quando você liga na central e solicita nossa equipe ou quando precisamos realizar alguma atividade preventiva, necessária para garantir sempre o melhor serviço.

Para sua segurança, quando agendar uma visita ou quando a gente entrar em contato para fazer um serviço de melhoria, utilize o aplicativo Minha Claro, assim você acompanha o deslocamento do técnico e ainda consegue verificar o nome completo e foto atualizada dele.

Ao recepciona-lo peça a ele para confirmar os dados, mas fique tranquilo nossos técnicos já fazem isso antes de entrar em sua casa.

Algumas pessoas podem receber uma ligação durante a visita alegando ser necessária a troca da senha do roteador, desligue! Quem faz essa configuração é o técnico que está ao seu lado.



Como funciona?

Alguns e-mails falsos copiam e-mails da conta digital, ou seja, fingem enviar faturas da Claro por e-mail. Essas mensagens podem conter tanto links maliciosos como faturas não verdadeiras anexadas.



Dica: Para se proteger, fique atento:

Nossos boletos só iniciam com 846 ou 848.

Nossas saudações iniciam sempre com o seu nome completo, não utilizamos saudações genéricas como “Cliente”, “Caro” ou “Prezado (a)”.

Confira todos os dados na sua fatura e boleto como : número de celular, plano, endereço e dados do titular.



Como funciona?

Uma empresa entra em contato com o cliente para oferecer instalação do serviço de Internet Fixa e cobra por esse serviço. Seja gerando um boleto falso ou solicitando dados do cartão de crédito para cobrança.



Dica: A Claro nunca solicita aos clientes o número do cartão de crédito para pagamentos, nem efetua cobrança de nenhum serviço por meio de débito em conta corrente ou boleto à parte. Toda cobrança de valores relativos a serviços solicitados pelo cliente é realizada exclusivamente em sua fatura.



Como funciona?

Os clientes recebem um SMS com links para atualização cadastral, desbloqueios, contestação de valores indevidos, etc.

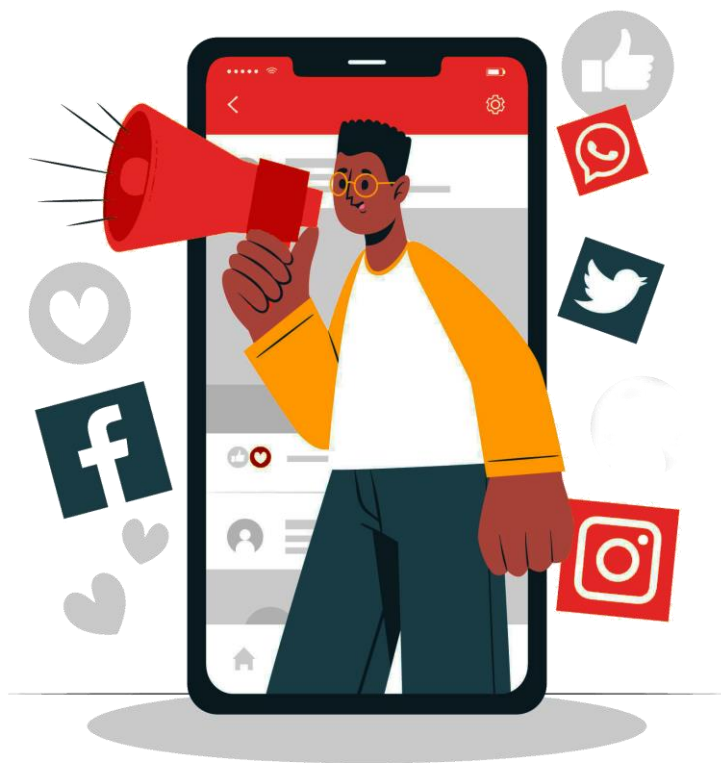


Dica: Nunca clique nesses links e/ou retorne as ligações para os números que enviam os SMS. Na dúvida, sempre procure o canal oficial da empresa (banco, operadora, loja).

Veja um exemplo de mensagem pirata:

“Fulano”, caso não tenha efetuado o pagamento da fatura 20/07/2020 – 102,50, pague com a numeração do código de barras: 8420000001-2 154200980001-4 11033302476-2 04645650510-1.

Não faça o pagamento, entre em contato com a empresa que estaria solicitando o pagamento deste débito através dos canais oficiais.



Como funciona?

Todo mundo já recebeu um SMS dizendo que ganhou prêmios e divulgando curas milagrosas. Mas fique atento: eles não são enviados pela Claro e, na verdade, são vendidos ilegalmente. Apenas empresas autorizadas pelas operadoras de telefonia móvel podem contratar o envio de SMS. Para saber se um SMS é oficial ou pirata, consulte no site "[SMS PIRATA](#)".

É fácil reconhecer essas mensagens. Confira, na comparação que fizemos, como diferenciar mensagens oficiais e piratas.



Dica: SMS oficial é enviado por empresas homologadas pelas operadoras e entregue de forma segura. Mensagens enviadas nos horários autorizadas pela Anatel, de números oficiais da Claro (geralmente compostos por 3 a 5 números)

Respeitam as regras estabelecidas pela Anatel e outros fóruns específicos que regulamentam o mercado, como o MEF (Mobile Entertainment Forum).

Veja um exemplo de SMS confiável:

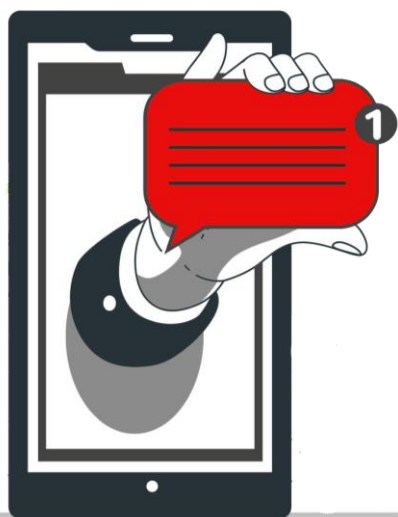
87-xxx

Prezado Cliente, registramos sua solicitação e entraremos em contato em até 48 horas.

Veja um exemplo de SMS pirata:

(81) 98125-xxxx

Parabéns você foi sorteado na promoção cliente da sorte! Para receber seu prêmio ligue: (81) 98125-xxxx

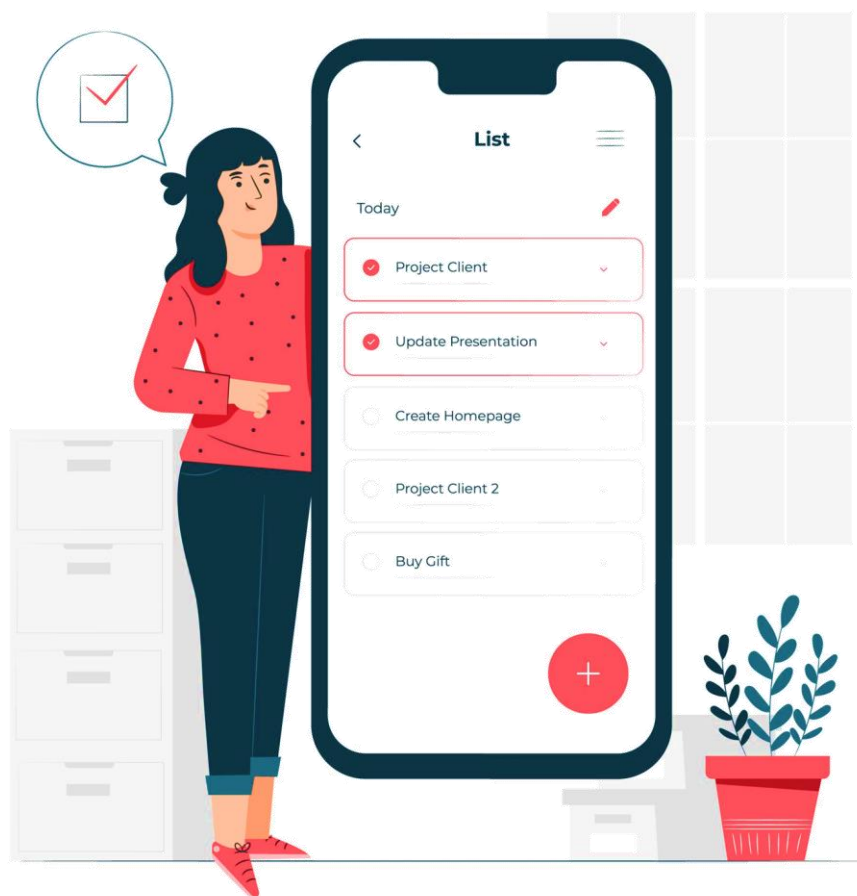


A Claro nunca envia comunicados de premiações via SMS nem utiliza números como (11) XXXX-XXXX para falar com os seus clientes. Para evitar que essas mensagens de texto sejam enviadas para você, seja cauteloso ao informar o número em sites e lojas, não divulgue seu número para estranhos e nunca retorne a ligação de números desconhecidos.

Como funciona?

O cliente recebe uma ligação informando que foi contemplado na promoção Recarga Premiada e receberá um SMS com o código da MINHA CLARO. Com o cliente em linha, o falso atendente pede para informar esse código e assim obtém acesso a todas as informações que constam na aplicação.

 **Dica:** É importante esclarecer que a Claro não solicita esse ou qualquer código e senhas. Até porque tais dados são pessoais, intransferíveis e não devem ser compartilhados nem mesmo com um atendente.



Como funciona?

Os golpistas se passam por parceiros e/ou funcionários da Claro para oferecer redução e/ou descontos na sua fatura. Após a confirmação de dados dos clientes, emitem boleto falso e orientam o pagamento.

A Claro não efetua esse tipo de ligação nem possui parcerias com empresas que oferecem serviços de redução de custos telefônicos. A sua fatura é enviada diretamente pela Claro para o endereço cadastrado, havendo a possibilidade de envio online caso você prefira. Consulte saldos e faturas usando o Minha Claro ou por meio do *10621 (ligação feita de celular).



Dica: É muito importante habilitar a “confirmação em duas etapas” do WhatsApp. Para isso, clique em “Configurações/Ajustes”, depois clique em “Conta” e depois em “confirmação em duas etapas”; habilitar senha de 6 dígitos numéricos.

JAMAIS compartilhe o código de 6 números que chegar por SMS.



Como funciona?

Bandidos criam sites falsos de venda de mercadoria (eletrônicos, eletrodomésticos, etc.). Este golpe costuma ter maior incidência em datas comemorativas e promocionais, como por exemplo, a Black Friday.

O golpista usa endereços de empresas famosas, alterando só o final do endereço eletrônico, bem como usam o layout dos sites conhecidos, tudo para ludibriar a vítima, fazendo-a pensar que se trata do site verdadeiro.



Dica: Observe com cuidado todo o endereço eletrônico.

Pesquise a reputação da empresa eletrônica em que pretende efetuar a compra.

Desconfie de objetos que estejam à venda por preço muito abaixo daquele praticado no mercado.



A maioria dos autores destes crimes, não se vestem mal, falam bem, tem boa aparência, geralmente não usam armas e podem estar atrás de uma tela de computador.

Caso tenha sofrido um golpe ou alguma transação suspeita relacionada a Claro, aja o mais rápido possível.

Para isso colocamos a sua disposição diversos canais, confira abaixo:

- > Utilize o canal csirt@claro.com.br
- > Consulte nossa página no **claro.com.br/seguranca**
- > Acesse nosso **App Minha Claro** para consultar boletos e dados de visitas técnicas.
- > WhatsApp **(11) 99991- 0621**
- > Ligue **1052 /10621**
- > Utilize o canal interativo ***1052#**
- > Envie um **SMS** com a palavra **Claro** para **1052**
- > Cliente **Claro Residencial** pode contar com atendimento exclusivo pelo **0800 721 00 27**
- > Ouvidoria Claro Residencial **0800 701 0180**
- > Ou caso prefira, pode ir a uma **loja Claro** e conversar com um de nossos atendentes.

**Segurança da Informação é
responsabilidade de todos.**

Claro