



CONNECTICUT PROTEÇÃO DO CONSUMIDOR NEWSLETTER MENSAL

Volume 2 / Edição 9 / Setembro de 2025

ALERTA DE GOLPE

O que é: Golpes de mensagem errada

Como funciona:

Golpistas mandam mensagem fingindo que entraram em contato com o número errado.

Uma conversa casual é iniciada para ganhar sua confiança e tentar roubar dados pessoais ou financeiros com truques e táticas de pressão.

Como se proteger:

Não responda nem clique em links enviados por quem você não conhece. Denuncie ou bloqueie o número.

Nunca envie dados pessoais ou financeiros, especialmente sem confirmar a identidade da pessoa.

GOLPES DE IDENTIDADE FALSA: VERDADE OU MENTIRA?

Os golpes de identidade falsa estão cada vez mais populares. Nos últimos meses, golpes comuns desse tipo incluem mensagens de texto avisando você sobre uma taxa não paga ou alegando que o destinatário não compareceu ao júri quando solicitado.

Os golpistas se passam por funcionários de vários setores: agências governamentais, suporte técnico, grandes varejistas e equipes de atendimento ao cliente. Em 2024, houve uma perda de **US\$ 2,95 bilhões** devido a golpes de identidade falsa nos Estados Unidos, [de acordo com a Federal Trade Commission \(Comissão Federal de Comércio\)](#).

Se você receber uma mensagem alegando ser de uma empresa, agência governamental ou equipe de atendimento ao cliente, considere estas perguntas ABC:

AÇÃO: alguma ação imediata é necessária? A pessoa está exigindo que você confirme sua conta ou pague um valor pendente?

BOTÃO: há algum botão que levará você para outro local? Um link, uma foto ou um anexo para download?

CONSEQUÊNCIA: a mensagem ameaça com uma consequência se a ação não for concluída? Sua conta ficará bloqueada? (Prisão, multas etc.)

Se a resposta para as perguntas for “SIM”, pode ser um golpe.

Esse tipo de golpe é chamado de “phishing” — o remetente se passa por uma pessoa ou organização conhecida alertando o destinatário sobre um problema falso e exigindo uma ação urgente. Ele vai intimidar o destinatário com uma consequência caso a ação não seja realizada.

Os golpistas recorrem a táticas de intimidação para convencer os destinatários a enviar dinheiro, informar dados pessoais ou clicar em links perigosos. **Se você receber uma mensagem como essa, não responda. Só denuncie e exclua.**

Alguns sinais de alerta adicionais de golpes de identidade falsa:

- Exigência de informações pessoais
- O e-mail termina com “@gmail.com”, “@yahoo.com” ou um domínio que não seja o nome da empresa



SOLICITAÇÕES DE PALESTRA

Deseja que o DCP (Departamento de Proteção ao Consumidor de Connecticut) palestre na sua organização ou participe do seu evento? Entre em contato com Catherine Blinder pelo e-mail Catherine.Blinder@ct.gov para enviar uma solicitação.

Fale conosco

Connecticut Department of Consumer Protection

450 Columbus Boulevard,
Suite 901

Hartford, CT 06103-1840

Linha principal: (860) 713-6100
(das 8h30 às 16h30)

Consumer Complaint Center (Centro de Reclamações do Consumidor)

(860) 713-6300

Ligação gratuita: (800) 842-2649

Das 8h30 às 16h30

E-mail: DCP.complaints@ct.gov

ACESSE NOSSA PÁGINA
CT.GOV/DCP

- A mensagem tem erros gramaticais e de digitação ou frases mal formuladas
- Solicitação para clicar em um link ou baixar um anexo para “ver mais informações ou documentos financeiros”
- Alguém liga para você alegando ser do “atendimento ao cliente” e pedindo a senha da sua conta ou sugerindo que você crie uma conta por telefone

Se você receber uma mensagem suspeita de um serviço que você utiliza com frequência, **não interaja com ela**. Para confirmar se o suposto problema é falso, entre em contato diretamente com a empresa.

Buscar “Número de atendimento ao cliente da [nome da empresa]” em um mecanismo de pesquisa pode levar a um número de telefone fraudulento.

Use o número de atendimento ao cliente encontrado no site da empresa, aplicativo, correspondência, verso do cartão de crédito etc.

Golpes de transferência de dinheiro

Golpes “Transfira para proteger” são cada vez mais comuns.

Perdas registradas por golpes de identidade falsa para adultos com 60 anos ou mais:

2020 — US\$ 55 milhões

2024 — US\$ 445 milhões

Alguém liga se passando por um banco, varejista ou agência governamental e avisa que há atividades suspeitas na sua conta e seu dinheiro está em risco. O golpista usa frases como:

“Seus dados estão sendo usados em atos criminosos”

“Seu computador foi hackeado” “Alguém está usando sua conta”

Para proteger seu dinheiro, eles incentivam você a transferi-lo para uma “conta de segurança” por criptomoeda (Apple Cash, caixa eletrônico de Bitcoin).

Em alguns casos, os golpistas alegam ser da Federal Trade Commission (FTC) e convencem as pessoas a entregar grandes quantias de dinheiro ou ouro a mensageiros.

Se você receber uma ligação desse tipo, desligue e denuncie o incidente em ReportFraud.ftc.gov

Esquecemos alguma dica? Algum assunto sobre o qual você gostaria de saber mais? Envie um e-mail para DCP.Communications@ct.gov.