BOLETÍN MENSUAL DE PROTECCIÓN AL CONSUMIDOR DE CONNECTICUT

Volumen 2 / Número 9 / Septiembre de 2025

ALERTA DE ESTAFA

De qué se trata: estafas basadas mensajes de texto a números equivocados

Cómo funcionan: los estafadores le envían mensajes de texto fingiendo haberse comunicado con un número equivocado.

Comienzan con una conversación casual para ganarse su confianza, luego intentan robar su información personal o financiera a través de trucos y tácticas de presión.

Cómo puede protegerse:

No responda ni haga clic en ningún enlace de alguien que no conoce y que le envíe mensajes de texto. Sea proactivo denunciando o bloqueando el número.

Nunca comparta información personal o financiera por mensaje de texto, especialmente si no ha verificado su identidad.

ESTAFAS POR SUPLANTACIÓN DE IDENTIDAD: ¿REALIDAD O FICCIÓN?

Las estafas de impostores son cada vez más populares. En los últimos meses, las estafas más comunes incluyen mensajes de texto que notifican sobre un peaje impago o que afirman que el destinatario no se presentó a su deber como jurado.

Los estafadores se hacen pasar por empleados de diversos sectores: agencias gubernamentales, soporte técnico, grandes minoristas y equipos de atención al cliente. En 2024, se registraron pérdidas de **$2,95 mil millones** debido a estafas por suplantación de identidad en Estados Unidos, según la Federal Trade Commission (Comisión Federal de Comercio).

Si recibe un mensaje que dice provenir de una empresa, una agencia gubernamental o un equipo de atención al cliente, pregúntese lo siguiente:

ACCIÓN: ¿Hay una acción inmediata? ¿La persona le pide que verifique su cuenta o pague un saldo?

BOTÓN: ¿Existe un botón para ocuparse de la ubicación? ¿Hay un enlace, foto o archivo adjunto para descargar?

CONSECUENCIA: ¿El mensaje amenaza con alguna consecuencia si no se completa la acción? ¿Se suspenderá su cuenta? (cárcel, multas, etc.)

Si responde “SÍ” a las preguntas anteriores, podría ser una estafa.

Este tipo de estafa se llama “fraude electrónico” o *phishing*: el remitente se hace pasar por una figura u organización conocida para alertar al destinatario de un problema falso y exigir una acción urgente. Intimidarán al destinatario con una consecuencia si esa acción no se completa.

Los estafadores utilizan tácticas de miedo para convencer a los destinatarios de que envíen dinero, completen información personal o hagan clic en un enlace dañino. **Si recibe un mensaje como este, ignórelo. En lugar de responder, márquelo como no deseado y elimínelo.**

Algunas señales de alerta adicionales de estafas por suplantación de identidad:

SOLICITUDES DE CHARLAS

¿Quiere que el DCP (Departamento de Protección del Consumidor de Connecticut) dé una charla en su organización o participe en su evento? Póngase en contacto con Catherine Blinder al correo electrónico Catherine.Blinder@ct.gov para enviar una solicitud.

Contacto

Connecticut Department of Consumer Protection
450 Columbus Boulevard,
Suite 901
Hartford, CT 06103-1840
Línea principal: (860) 713-6100
(de 8:30 a. m. a 4:30 p. m.)

Consumer Complaint Center (Centro de reclamos del consumidor)
(860) 713-6300
Línea gratuita: (800) 842-2649
De 8:30 a. m. a 4:30 p. m.
Correo electrónico:
DCP.complaints@ct.gov

VISÍTENOS EN LÍNEA

CT.GOV/DCP

- Solicitud insistente de información personal.
- El correo electrónico termina con “@gmail.com”, “@yahoo.com” o un dominio distinto al nombre de la compañía.
- Hay errores tipográficos, errores gramaticales o lenguaje extraño.
- Se le solicita hacer clic en un enlace o descargar un archivo adjunto para "ver más información o documentos financieros".
- Si una persona lo llama, dice ser de “atención al cliente” y le pide la contraseña de su cuenta o le sugiere crear una nueva cuenta por teléfono.

Si recibe un mensaje sospechoso de un servicio que utiliza habitualmente, **no interactúe con él**. Para confirmar que el supuesto problema es falso, comuníquese directamente con la compañía.

Si busca “número de atención al cliente de [nombre de la compañía]” en un motor de búsqueda, es posible que lo dirijan a un número de teléfono fraudulento.

Utilice el número de atención al cliente que se encuentra, entre otros, en el sitio web, la aplicación, comunicaciones por correo o el reverso de la tarjeta de crédito de la compañía.

Estafas basadas en "Transferir para proteger"

Las estafas de "Transferir para proteger" están en aumento en EE. UU.

Pérdidas denunciadas debido a estafas de suplantación de identidad para adultos de 60 años o más:

2020: $55 millones

2024: $445 millones

Una persona que se hace pasar por un banco, un comercio o una agencia gubernamental le notifica que hay actividad sospechosa en su cuenta y que sus finanzas están en riesgo. La persona que llama puede usar frases como:

"Su identificación está siendo utilizada en actividades delictivas"

"Su computadora ha sido hackeada" "Alguien está usando su cuenta"

Para proteger su dinero, le instan a transferir dinero a una "cuenta segura" mediante criptomonedas (Apple Cash, cajeros automáticos de Bitcoin).

En algunas denuncias, los estafadores afirmaron ser de la Federal Trade Commission (FTC) y convencían a las personas de entregar fajos de dinero en efectivo u oro a los mensajeros.

Si recibe una llamada similar, cuelgue y denuncie el incidente en ReportFraud.ftc.gov.

¿Se nos pasó por alto algún consejo? ¿Hay algún tema sobre el que desee obtener más información? Envíenos un correo electrónico a DCP.Communications@ct.gov.