



BOLETÍN MENSUAL DEL CONNECTICUT CONSUMER PROTECTION

Volumen 1 / Número 2 / octubre de 2024

ALERTA DE ESTAFA

Qué son: Estafas laborales.

Cómo funcionan: Los estafadores ofrecen trabajos a tiempo completo o temporarios a distancia con la promesa de que se pueden ganar cientos de dólares a la semana. Cuando acepta el trabajo, le solicitan información personal, como su número del seguro social e información bancaria, para "depositar sus ganancias".

Cómo puede protegerse:

No responda ni acepte mensajes de números desconocidos. Bloquee e ignore a los estafadores y evite todo tipo de interacción con ellos. Antes de aceptar un puesto de trabajo, investigue la empresa o el reclutador para asegurarse de que sea real.

Todo lo que necesita saber para estar seguro este Halloween.

- Use disfraces confeccionados con telas resistentes al fuego, como poliéster o nailon.
- Aunque su disfraz esté confeccionado con una tela resistente al fuego, tenga cuidado con las llamas.
- Lleve un disfraz brillante y reflectante o añada tiras de cinta reflectiva para ser más visible y lleve una linterna o bastones luminosos cuando salga a pedir golosinas.
- Compruebe que las caretas se ajusten bien, que permitan una ventilación adecuada y que los orificios para los ojos sean lo suficientemente grandes como para garantizar una visión completa. En su lugar, lo ideal es ponerse maquillaje y un sombrero.
- Pruebe el maquillaje del disfraz al menos dos días antes, en un brazo, no en la cara, y si aparece una erupción, enrojecimiento, hinchazón u otros signos de irritación, no lo utilice.
- No coma las golosinas hasta que las hayan revisado en casa.
- Revise las etiquetas para detectar alérgenos alimentarios.
- Indique a los niños que no acepten, ni coman, nada que no esté presentado en un envoltorio comercial. Reparta únicamente golosinas preenvasadas y con envoltorio comercial.
- Deseche todo lo que parezca sospechoso o que se haya abierto accidentalmente o cuyo envoltorio estuviese roto cuando lo recibió.
- Mantenga refrigerados todos los alimentos perecederos hasta el momento de servirlos. No coma bocadillos que lleven mucho tiempo servidos en una fiesta.
- Tenga cuidado con la decoración, para no crear obstáculos o peligros que puedan hacer tropezar a alguien.



SOLICITUDES DE CHARLAS

¿Desea que el DCP dé una charla a su organización o presente una mesa 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 (860) 713-6300

Línea gratuita: (800) 842-2649
De 8:30 a. m. a 4:30 p. m.

Dirección de correo electrónico:
DCP.complaints@ct.gov

VISÍTENOS EN LÍNEA CT.GOV/DCP

REGÍSTRESE AHORA PARA EL SIMPOSIO ANUAL SOBRE COMUNICACIÓN INTERCULTURAL DEL 25 DE OCTUBRE

El futuro es hoy: la IA en la política y el bien públicos es el tema del 8.º simposio anual sobre comunicación intercultural del Department of Consumer Protection (DCP, Departamento de Protección al Consumidor). El simposio de 2024 se llevará a cabo el 25 de octubre, de 8:30 a. m. a 4:00 p. m., en el Connecticut Convention Center ubicado en 200 Columbus Boulevard en Hartford, Connecticut. Regístrese ahora en portal.ct.gov/DCP/Symposium.

Es el mes de la concientización sobre ciberseguridad. ¿Ha cambiado sus contraseñas?

Ahora es un buen momento para asegurarse de que su mundo en línea esté protegido. A continuación, se indican algunas medidas sencillas que puede adoptar para mantener la seguridad de su información:

1. **Reconozca el fraude electrónico de suplantación de identidad o phishing y denúcielo:** reconozca los correos electrónicos de phishing por el uso de lenguaje alarmante u ofertas demasiado buenas para ser ciertas. No haga clic en enlaces de correos de este tipo ni responda a estos. Denuncie el intento de fraude electrónico y elimine los mensajes.
2. **Utilice contraseñas seguras:** procure que sus contraseñas tengan al menos 16 caracteres, sean aleatorias y únicas para cada cuenta. Utilice un gestor de contraseñas que mantenga, cree y guarde contraseñas seguras, y le avise si alguna se encuentra comprometida.
3. **Active la autenticación multifactor (AMF):** utilice la AMF en los sitios que la ofrezcan. La AMF proporciona una capa adicional de seguridad para iniciar sesión en cuentas y aplicaciones; por ejemplo, con reconocimiento facial o con un código que se envía por mensaje de texto.
4. **Actualice el software:** cuando los dispositivos, aplicaciones o programas envían notificaciones de actualizaciones disponibles, conviene instalarlas lo antes posible. Las actualizaciones solucionan errores de los códigos de seguridad para una mayor protección de sus datos. Active las actualizaciones automáticas para que sea aún más fácil.

¿Se nos pasó algún consejo? ¿Quiere saber más sobre algún tema?
Envíenos un correo electrónico a DCP.Communications@ct.gov.