Estafas de impostor

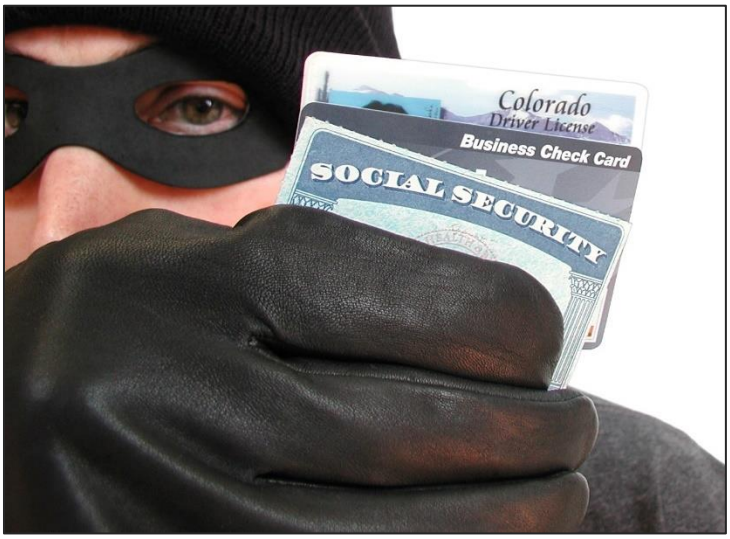
¡Ten cuidado! ¡Los impostores están por todos lados! ¿Cuándo suena el teléfono, sabe quién está llamando antes de contestar o quién envió el correo que acaba de abrir? ¿Cuándo usa su computadora o teléfono inteligente, sabe quién mandó el correo eléctrico que está en su bandeja de entrada? ¿Sabe quién creó el mensaje emergente que aparece en su pantalla? Todos estos métodos y muchos más se utilizan por estafadores quienes no son lo que parecen ser.

La mejor defensa contra las estafas de impostor es no responder.

Señales de una estafa de impostor

Aquí están algunos indicadores comunes de que está lidiando con un impostor:

- **Solicitudes de información personal. Algunos** ejemplos incluyen: fecha de nacimiento, número de Seguro Social, número de identificación de Medicare, números de tarjeta de crédito o de cuentas bancarias.
- **Solicitudes de cualquier tipo de pago.** Ningún ganador de un concurso, premio o beca tiene que hacer pagos para recibir sus ganancias o premio.
- **Solicitudes de pago con criptomonedas, envío de dinero, tarjetas de débito prepagadas, o transferencias bancarias.** Proporcionar dinero a través de cualquiera de estos métodos es lo mismo que dar a alguien dinero en efectivo y no es probable que pueda ser rastreado o recuperado una vez dado.
- **Amenazas y urgencia.** Entre más amenazante la llamada – será arrestado, tendrá que ir al juicio, su crédito estará arruinado – más probable es que venga de un impostor. Las llamadas que requieren acción urgente de alguien que no conoce, probablemente son hechas por impostores.
- **Solicitudes de discreción.** Esto es especialmente cierto para las solicitudes de asistencia financiera de parientes que dicen “No le diga a mi mamá o papá.” O para llamadas sobre ganar un premio donde el llamador le dice que “no le puede contar a nadie hasta que reciba sus ganancias.”



Estafas telefónicas de impostor

- **IRS o Departamento del Tesoro.** Llamadas amenazando con que tiene que pagar infracciones tributarias ahora. **El IRS nunca se pondrá en contacto con usted por teléfono. Le contactará por correo. No harán amenazas.**
- **Subvenciones Federales.** No se deje engañar por el código de área 202 que hace parecer que la llamada viene de Washington, D.C. Estas subvenciones no solicitadas no se galardonan. En el caso improbable de que alguien reciba una subvención que no solicitó, **no se requiere ningún pago para recibir la subvención.**
- **Medicare o la Ley de Cuidado de Salud Asequible.** El llamador dice ser un representante del gobierno insistiendo que le proporcione información de identificación personal y/o pague una cuota o enfrente la pérdida de beneficios. Las **agencias gubernamentales se pondrán en contacto con usted por correo, no por teléfono. No harán amenazas por teléfono.**
- **Otras Autoridades de Aplicación de la Ley o Agencias Gubernamentales.** El llamador podría

amenazar con deportación, pero que por una tarifa le ayudará a conseguir su certificación. Esperan que tenga suficiente miedo como para desprenderse del dinero y/o información de identificación personal. O un llamador podría decir que un dignatario extranjero, que necesita su ayuda con una transferencia de dinero, es "legítimo". **Ninguna autoridad de aplicación de la ley ni agencia gubernamental hace ese tipo de llamadas.**

- **Ganador de la Lotería o un Premio.** El llamador dice que usted ha ganado, pero hay que pagar un cargo administrativo, envío o impuestos. **Usted nunca tiene que pagar por un premio o ganancias.**
- **Asistencia Familiar.** También conocido como "Estafa de los Abuelos". Estos llamadores se aprovechan de la buena voluntad y el deseo de ayudar a la familia. El llamador dirá que es un miembro de la familia, usualmente uno más joven, que está en problemas y necesita asistencia financiera inmediata. Estos estafadores se alimentarán de la información que se les da inadvertidamente. **El llamador le pedirá que no llame a alguien que podría verificar la legitimidad de la llamada** ("No le llame a mamá o papá") y que envíe dinero de una manera no rastreable.
- **Problemas de Computadora.** El llamador dice ser un representante de "Microsoft" o "Google" u otra compañía conocida, y dice que ha detectado un problema con su computadora. El llamador podría decirle que busque en un lugar específico de su computadora donde verá muchos mensajes de error. El llamador le dirá que esto es resultado de un virus u otro problema con su computadora. **Los mensajes de error que usted ve son completamente normales en cualquier computadora que funciona adecuadamente.** Estos llamadores intentarán hacerle pagar por servicios, probablemente por tarjeta de crédito y que les dé acceso a su computadora para que puedan robar información personal y descargar software dañino conocido como "malware" que continuará permitiendo el acceso a su computadora y el control de esta. Las compañías legítimas no hacen estos tipos de llamadas. **Nunca le dé acceso a su computadora a un llamador, a menos que esté seguro de que sabe quién está al otro lado del teléfono.**
- **Servicios Públicos Cortados.** El llamador dice que usted no ha pagado su factura de servicios públicos y que alguien está en camino para desconectar los servicios a menos que haga un pago inmediato al llamador. Estas llamadas se enfocan en empresas pequeñas pero algunos consumidores han reportado recibir estas llamadas en casa. Para verificar si lo que dice el llamador es cierto, **llame al número que está en su factura, no el número que el llamador le da.**
- **Números "Spoofed".** Existe tecnología que permite a un llamador controlar lo que parece en el identificador de llamadas. Esto se llama **"spoofing"**. Las llamadas pueden aparecer como llamadas de una agencia gubernamental, compañía o hasta un vecino, cuando en realidad las llamadas vienen desde fuera del país. **Si no reconoce el número que aparece en el identificador de llamadas, deje que la llamada vaya a su contestador automático o buzón de voz.** Si es importante o una llamada personal, el llamador dejará un mensaje. Si tiene una pregunta sobre el mensaje dejado, llame a la línea directa de Protección al Consumidor al (800) 422-7128.

Existe tecnología de inteligencia artificial que permite a la persona que llama utilizar una computadora para imitar la voz de otra persona. Una computadora necesita tan solo unos segundos de audio para hacer esto.

Estafas de impostor por correo

Las estafas por correo requieren una respuesta una vez que haya recibido el correo. Las estafas más comunes de impostor son las estafas de premios donde se le instruye que llame y se le dice que tiene que hacer un pago de algún tipo para recibir sus ganancias. Otras versiones de las estafas de impostor telefónicas también pueden llegar por el correo o correo electrónico.

Estafas de impostor por computadora

- **Estafas de Correo Electrónico.** Las estafas por correo electrónico pueden ser versiones de las estafas de impostor por teléfono o correo. A menudo, el objetivo puede ser conseguir que haga

clic en un enlace que le pedirá información personal o hacer clic en un archivo adjunto que descargará un virus u otro malware en su computadora.

- **Mensajes Emergentes.** Un mensaje aparecerá en su pantalla, usualmente afirmando que hay algún problema con su computadora y diciéndole que haga clic en la ventana para recibir asistencia. Luego, se le dará información para ponerse en contacto con alguien que le ayude, posiblemente de una compañía conocida como "Microsoft" o "Google". Esto es una variación de las llamadas de problemas de computadora. A menudo, los mensajes de emergentes son el resultado de un virus que ha sido descargado en su computadora para hacerle poner en contacto con ellos en vez de llamarle a usted directamente. A veces podría recibir una llamada cuando aparece este mensaje, o hace clic en la ventana emergente. Si aparece un mensaje de error en su computadora, póngase en contacto con alguien que conoce y confíe para ayudarle. No haga clic en las ventanas emergentes reportando un problema con su computadora.
- **Estafas de Impostor de Búsqueda en Línea.** Cuando busca asistencia por medio de una búsqueda en línea, sea consciente de que algunas compañías, incluyendo estafadores, han pagado para tener sus enlaces en la parte superior de la lista de búsqueda. Es muy fácil pensar que usted está hablando con un representante de la compañía real que usted quiere, o que está en su sitio web, solo para encontrarse con que se le están pidiendo que proporcione información personal, información de pago, y/o acceso a su computadora. Verifique la dirección web para asegurarse de que usted está lidiando con la compañía real.
- **Estafas de Impostor de Citas en Línea. Las** citas en línea hacen que sea más fácil para una persona mentir sobre sí misma. Suelen ser utilizadas fotos falsas o anticuadas, historias personales mejoradas y exageradas o rasgos personales inventados. Con las citas tradicionales es posible hablar con amigos, familiares o conocidos para comprobar la reputación de una persona. Las citas en línea usualmente hacen esto imposible. Una vez que un estafador está seguro de que tiene su confianza, empezará a pedir dinero. Tal vez le dirá que lo necesita para conseguir el dinero que el gobierno le debe, cubrir el costo de una enfermedad repentina, cirugía, un robo, accidente o pérdida de empleo. Podría ser para él, o una hija o un hijo. Podría pedir dinero para cubrir los costos del viaje para conocerse por fin cara a cara. Podría recibir documentos de un abogado como "prueba" de sus intenciones genuinas junto con la promesa de devolver el dinero. **Por más real que parezca la relación, es una estafa y usted perderá el dinero enviado.**
- **Estafa de Impostor de las Redes Sociales.** Trate a los enlaces en mensajes en estos sitios como si fuera un enlace en un correo electrónico. Si parece sospechoso, aunque conozca la fuente, es mejor borrarlo o marcarlo como basura. Los estafadores pueden entrar en las cuentas y enviar mensajes que parecen que son de sus amigos, pero no lo son. Si sospecha que un mensaje es fraudulento, utilice un método alternativo para ponerse en contacto con su amigo para averiguarlo. No confíe en que un mensaje realmente es de quien dice ser.

¡No responda!

La mejor defensa en contra de todas estas estafas de impostor es no responder.

- **No conteste la llamada.** Utilice su identificador de llamadas. Si no reconoce el número deje que la llamada se vaya a su contestador automático o buzón de voz. Si contesta la llamada, cuelgue tan pronto como se dé cuenta de que esta no es una persona con quien desea hablar. Hablar con estos llamadores o regresar la llamada probablemente resultará en contactos adicionales de ellos y otros estafadores.
- **Borre los correos electrónicos de remitentes desconocidos.** Si no sabe quién lo envió, no lo abra. A veces abrir un correo electrónico es suficiente para informar a un estafador que eso es una dirección válida y ellos continuarán enviándole correos electrónicos. **Si usted no sabe quién lo envió, nunca haga clic en un enlace o archivo adjunto en un correo electrónico.**
- **Verifique el resultado de su búsqueda.** Antes de actuar según el resultado de una búsqueda en línea, verifique para asegurarse de que usted está

lidiando con la compañía que desea. **Si se pone en contacto, esté atento a los signos de una estafa.**

- No llame al número de verificación que se le da. Llame al número que está en su factura, que se encuentra en el directorio telefónico o en un directorio fiable en línea. **Nunca verifique si algo es legítimo utilizando el número que le dan por teléfono, correo, correo electrónico o mensaje**.

Para más información, o para presentar una queja, visite nuestro sitio web o contáctese con:

Departamento de Agricultura, Comercio y Protección al Consumidor de Wisconsin
Departamento de Protección al Consumidor
2811 Agriculture Drive, PO Box 8911
Madison, WI 53708-8911

Correo electrónico: DATCPHotline@wi.gov
Sitio web: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

ImposterScams214 (rev 1/24)