BUREAU OF CONSUMER PROTECTION Consumer Facts

Protecting Wisconsin Consumers for 75 Years

Estafa de Impostor

¡Ten cuidado! ¡Los impostores están por todos lados! ¿Cuándo suena el teléfono, sabe quién está llamando antes de contestar o quien envió el correo que acaba de abrir? ¿Cuándo en su computadora o teléfono inteligente, sabe quién mando el correo eléctrico que este en su bandeja de entrada? ¿Sabe quien 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.

Señales de una estafa de impostor

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

- **Solicitudes para información personal.** Ejemplos incluyen: fecha de nacimiento, número de Seguro Social, número de identificación de Medicare, números de tarjeta de crédito o de cuentas bancarias.

- **Solicitudes para 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 por enviar dinero o tarjetas de débito pre-pagadas.** Proporcionar dinero a través de cualquiera de estos dos métodos es lo mismo que dar a alguien dinero en efectivo y no es probable que pueda ser rastreado o se recupera una vez dado.

- **Amenazas y urgencia.** Entre más amenazante la llamada-estará arrestado, tener que ir al juicio, su crédito estará arruinado-lo más probable es que viene de un impostor. Llamadas requiriendo acción urgente de alguien que no conoce, probablemente se hacen por impostores.

- **Solicitudes para discreción.** Esto es especialmente cierto para las solicitudes de asistencia financiera de parientes que dicen “No le diga a mi mama o papa.” O para llamadas sobre ganar un premio donde el llamador le dice que no se le puede contar a nadie hasta que reciba sus ganancias.

Estafas telefónicas del Impostor

- **IRS o Departamento del Tesoro.** Llamadas amenazantes que tiene que pagar ahora para infracciones tributarias. **El IRS nunca se pondrá en contacto con usted por teléfono. Le contactará por correo. No harán amenazas.**

- **Premio subvención Federal.** No se deje engañar por el código de área 202 que se hace parecer que la llamada viene de Washington, D.C. Estas subvenciones no solicitadas no se galardona. En el caso improbable de que alguien recibe 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 se le proporciona información de identificación personal y/o pagar una cuota o enfrentar la pérdida de beneficios. **Agencias gubernamentales se pondrán en contacto con usted por correo, ni por teléfono. No harán amenazas por teléfono.**

- **Otro Aplicación de la Ley o Agencia Gubernamental.** El llamador podría amenazar

deportación pero por una tarifa le ayudara a conseguir su certificación. Esperan que tendrá bastante 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 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 no llamar a alguien quien podría verificar la legitimidad de la llamada** ("No le llame a mama o papa") y enviar 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 buscar 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, probable por tarjeta de crédito y para obtener acceso a su computadora para que puedan robar información personal y descargar software dañino conocido como "malware" que continuará permitiendo acceso a y control de su computadora**.** Ninguna de estas compañías 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 negocios pequeños pero algunos consumidores han reportado recibir estas llamadas en casa. Para verificar si lo que dice el llamador es cierto, **llame el número que está en su factura, no el número que el llamador le da.**

- **Números "Spoofed".** Hay tecnología que existe que permite a un llamador controlar lo que parece en el identificador de llamadas. Esto se llama **"spoofing"**. Llamadas pueden aparecer venir 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 se 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 dejada, llame a la línea directa de Protección al Consumidor al 1-800-422-7128.

Estafas Impostor de Correo

Estafas de 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 llamar y se le dice que tiene que hacer un pago de algún tipo para recibir sus ganancias. Versiones de las estafas de impostor telefónica también pueden pasar por el correo o correo electrónico.

Estafas Impostor de Computadora

- **Estafas de correo electrónico.** Estafas de correo electrónico pueden ser versiones de las estafas impostor de 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 se descargará un virus u otro malware en su computadora.

- **Pantallas emergentes.** Un mensaje aparecerá en su pantalla, usualmente afirmando que hay algún problema con su computadora y diciéndole hacer clic en la ventana para asistencia. Luego, se le dará información 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 problema de computadora. A menudo, los mensajes de las pantallas emergentes son el resultado de un virus que ha sido descargado en su computadora para hacerle ponerse en contacto con ellos en vez de llamar a usted directamente. A veces podría recibir una llamada una vez que aparezca este mensaje, o haga clic en la ventana emergente. **Si aparece un mensaje de error en su computadora, póngase en contacto con alguien que conoce y confié para ayuda.** No haga clic en las ventanas emergentes reportando un problema con su computadora.

- **Estafa impostor de búsqueda en línea.** Cuando buscando asistencia por medio de una búsqueda en línea, sea consiente que algunas compañías, incluyendo estafadores, han pagado para tener sus enlaces aparecer 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 está en su sitio internet, solo para averiguar que se le están pidiendo proporcionar información personal, información de pago, y/o acceso a su computadora. **Verifique la dirección web para asegurar que usted está lidiando con la compañía real.**

- **Estafas impostor de citas en línea.** Citas en línea se le hace más fácil para una persona para tergiversar sí mismo. Fotos falsas o anticuadas pueden ser utilizados, historias personales mejoradas y exageradas o rasgos personales fabricados. Con las citas tradicionales es posible hablar con los amigos, familiares o conocidos para comprobar la reputación de una persona. Citas en línea usualmente hace esto imposible. Una vez que un estafador está seguro 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 genuinos junto con la promesa de devolver el dinero. **Tan real como parezca la relación, es una estafa y usted pierde el dinero enviado.**

- **Estafa 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 hackers pueden entrar en las cuentas y enviar mensajes que parecen que son de tus amigos, pero no lo son. Si sospecha que un mensaje es fraudulenta, utilice un método alternativo para ponerse en contacto con su amigo para averiguarlo. **No confié en que un mensaje realmente es de quien dice.**

¡No Responde!

La mejora defensa en contra 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 que esto no es una persona con quien desea hablar. Hablando con estos llamadores o regresando la llamada probablemente resultará en contactos adicionales de ellos y otros estafadores.

- **Borre 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 valido 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 en el resultado de una búsqueda en línea, verifique para asegurar 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 se les da por teléfono, correo, correo electrónico o mensaje**.

Contáctenos

Para más información, o para presentar una queja, visite nuestra página web o comuníquese con el Departamento de Protección al Consumidor.

Departamento de Protección al Consumidor
2811 Agriculture Drive
PO Box 8911
Madison WI 53708-8911

CORREO ELECTRÓNICO:
DATCPHotline@wi.gov

SITIO DE INTERNET:
datcp.wi.gov

(800) 422-7128

FAX: (608) 224-4677

TTY: (608) 224-5058

I:\dtcp\common\Fact Sheets\ImposterScamsSPANISH886 04/18