[Sello]
CIUDAD DE EUGENE
ESTADO DE OREGÓN
1830
POLICÍA

Departamento de Policía de la Ciudad de Eugene
(*City of Eugene Police Department*)
Equipo de participación comunitaria
INTEGRIDAD. COMPASIÓN. VALENTÍA.

Estafas y fraudes

Los delincuentes elaboran continuamente nuevas estafas dirigidas a separarlo de sus ahorros. Lo hacen engañándolo para que les proporcione, de cualquier manera posible, su efectivo, su identificación personal, sus números de cuenta corriente y su información de tarjetas de crédito. Si alguna persona le pide su efectivo, sus números de tarjeta de crédito u otra información personal –especialmente si usted no lo conoce bien- lo más seguro es negarse a lo que pide y verificar con la policía. La siguiente lista incluye algunas de las estafas más comunes que hemos observado en nuestra zona, pero siempre surgen inesperadamente nuevos tipos de estafa:

Estafa de examinadores de fraude bancario – En esta estafa, usted recibe una llamada de un supuesto profesional de los cuerpos policiales o un examinador de fraudes bancarios con su banco, quien le asegura que está investigando a un empleado y necesita su ayuda: que retire algo de dinero y se lo pase al examinador, con el propósito de un seguimiento. Desde luego, nunca más verá el dinero.

Estafas de loterías extranjeras – Ningún país extranjero se esforzará excesivamente por darle su dinero a una persona en el extranjero, ¡y es mucho menos probable si nunca ha comprado un número de lotería!

Estafas de "dinero encontrado" – Una persona asegura que encontró dinero, y mucho. Dicha persona quiere que usted se quede con el mismo mientras encuentra al dueño, pero primero deberá darle algo de dinero en efectivo para que pueda tenerle más confianza. Una vez que esto sucede, intercambia bolsas dejándolo con un saco lleno de documentos sin valor.

Estafas de "hágase rico" – Estas incluyen los esquemas piramidales, las estafas de inversión u otras estafas de "hágase rico de la noche a la mañana". Si parece demasiado para ser verdad, es porque generalmente no es verdad en absoluto.

Estafas de tarjetas regalo – La Comisión Federal de Comercio (*Federal Trade Commission*, FTC) nos recuerda que "las tarjetas regalo son una manera popular y conveniente de hacerle un regalo a alguien. También son una manera popular en la que los estafadores le pueden robar dinero. Es por eso que las tarjetas regalo son como efectivo: si compra una tarjeta regalo y alguien la utiliza, probablemente no recuperará su dinero. Las tarjetas regalo son para regalar, no pagar. Toda persona que exija el pago con una tarjeta regalo siempre es un estafador". Para obtener información adicional sobre las estafas de tarjeta regalo, visite el sitio web de FTC: https://www.consumer.ftc.gov/articles/paying-scammers-gift-cards.

Estafas de una buena causa – El delincuente asegura de manera fraudulenta que representa a una buena causa –por ejemplo, viudos, huérfanos, policía o bomberos- y pide dinero. O tergiversa un producto de limpieza u ofrece la venta de suscripciones a revistas que nunca da resultados. Con frecuencia, se supone que las ventas ayudan a una causa que vale la pena apoyar: mandar a los niños a un campamento o apoyar un centro de rehabilitación. Estas pueden llevarse a cabo yendo de puerta en puerta, por teléfono o por Internet.

Estafas de mejoras del hogar – Esto se trata comúnmente de una persona que llama a su puerta porque notó que es necesario reparar el techo o la entrada para el auto. Dicha persona le asegura que trabaja en el vecindario y le sobran materiales, así que puede ofrecerle un buen precio, pero usted deberá decidir inmediatamente. Una vez que esa persona tenga su dinero, desaparecerá o cubrirá su entrada para el auto con algo que no la mejore para nada.

Estafas nigerianas – No hay ningún viudo, huérfano, ministro de petróleo o cualquier otra persona en el extranjero que vaya a contactarse legítimamente con un desconocido y darle millones de dólares. Esto incluye la carta nigeriana o el fraude "419", en que promete que se le reembolsarán todos los gastos, tan pronto como se transfieran los fondos de Nigeria.

Estafas de familiares en situaciones de emergencia – Estas incluyen generalmente una variación de lo siguiente: "Soy tu sobrino, nieto, etc., que no has visto hace mucho tiempo, eres mi última esperanza, estoy metido en un gran lío, no se lo digas a mis padres, solo transfiere algo de dinero o me encerrarán y tirarán la llave". Pista: ¡la persona que llama NO es un familiar que no haya visto hace mucho tiempo, ni ninguna otra persona que conozca!

Estafas de romance – Aunque muchas personas se conocen legítimamente por medio de servicios de citas y salas de chat, no faltan los estafadores que se ocupan de este sector. Es posible que coloquen una fotografía, biografía o edad falsa y es prácticamente imposible confirmar o refutar su exactitud. Luego, inventan una convincente historia de infortunio que hará que usted se sienta honrado enviando dinero, sin darse cuenta de que lo han estafado. ¡En algunos esquemas más elaborados, dichos estafadores irán a vivir con usted, solo para sacarle el dinero de otras maneras una vez que hayan llegado!

Hay muchas más estafas que las descritas anteriormente y es posible que traten de comunicarse con usted por correo electrónico. Estos son algunos ejemplos:

Correos electrónicos para obtener información personal (*phishy*) – La forma más común de "obtener información personal" incluye correos electrónicos que pretenden ser de un minorista, organización, agencia gubernamental o banco legítimo. El remitente le pide que "confirme" su información personal debido a un motivo inventado: se está por cerrar su cuenta, se ha colocado una orden por algo en su nombre o se ha perdido su información debido a un problema de la computadora. ¡Otra táctica que utilizan los "ciberdelincuentes" es decir que son del departamento de fraudes de compañías conocidas y pedirle que verifique su información porque sospechan que usted puede haber sido una víctima de robo de identidad! En uno de los casos, un ciberdelincuente aseguró que pertenecía a una comisión estatal de loterías y le pedía a personas su información bancaria para depositar lo que habían "ganado" en sus cuentas.

No haga clic en enlaces dentro de correos electrónicos que le pidan su información personal – Los estafadores utilizan estos enlaces para atraer a personas a sitios web falsos que parecen ser los sitios reales de la compañía, organización o agencia por la que se hacen pasar. Si sigue las instrucciones e introduce su información personal en el sitio web, se la entregará directamente en las manos de ladrones de identidad. Para verificar si el mensaje es realmente de la compañía o agencia, llámela directamente o vaya a su sitio web (utiliando un buscador para encontrarla). No haga clic en adjuntos de correos electrónicos que no esté esperando, aunque sean de personas que conozca (o que parezcan ser de personas en sus contactos: a veces se "falsifican" direcciones electrónicas para que parezcan ser de sus contactos). Muchos de los virus están relacionados con tipos específicos de sitios web, particularmente aquellos que presentan material pornográfico. ¡Manténgase alejado de los sitios de pornografía y reducirá su riesgo! Además, tenga en cuenta que, aunque no le pidan información personal, es posible que planten un virus para los fines del *pharming*.

Cuidado con el *pharming* – Es una práctica fraudulenta en la que se desvía a los usuarios de Internet a un sitio web falso, el cual parece ser igual a uno legítimo, para obtener datos personales como contraseñas, números de cuenta, etc.

Llamadas telefónicas para obtener información personal (*phishy*) – Algunos estafadores lo llaman por teléfono para intentar convencerlo de que proporcione información personal, a fin de utilizarla para generar cargos en sus tarjetas de crédito. Una estafa que han experimentado algunos hoteles es cuando reciben llamadas en recepción pidiendo que los transfieran a un cuarto determinado. Luego, el estafador pretende ser el empleado de recepción, que tiene problemas con su tarjeta de crédito, y le pide que repita el número, inclusive el código de seguridad.

Cuidado con el *vishing* – Es la práctica fraudulenta de hacer llamadas telefónicas o dejar mensajes, asegurando que se es de compañías respetables, a fin de engañar a una persona para que revele datos personales como números bancarios o de tarjeta de crédito.

Inscríbase en el registro nacional de "no llamar". ¡Es fácil y gratuito! Llame al (888) 382-1222, dispositivo de telecomunicaciones para personas con pérdida auditiva (*TTY*, por sus siglas en inglés) (866) 290-4236, desde el número telefónico que desea registrar. Desafortunadamente, registrarse por teléfono puede no funcionar si vive en un complejo residencial que utilice un sistema telefónico de intercambio privado de sucursales (*PBX*, por sus siglas en inglés). Sin embargo, también puede registrarse en línea, en www.donotcall.gov. Si no tiene una computadora, utilice la de otra persona. Necesitará acceso a Internet y una dirección electrónica operativa. El sistema de "no llamar" enviará una respuesta a esa dirección con un enlace, al que se debe hacer clic dentro de un período de 72 horas, para completar el registro.

Si le interesa algún tema, solicite que le envíen información por escrito. NO les proporcione ninguna información personal. Verifique con la policía u otras fuentes fiables.

¡Cuando tenga alguna duda, siempre verifíquelo! Si está en peligro inmediato, llame al 911. Si el delincuente llama a su puerta, en la zona incorporada de Eugene, llame a la asistencia de rutina de la policía de Eugene, al 541-682-5111.