

Estafas por correo electrónico

OnGuard Online

Consejos de filtrado: 10 estafas que puede eliminar de su correo electrónico

Algunos usuarios de correo electrónico han perdido dinero en ofertas falsas que les llegan como mensajes no solicitados a su buzón. Los estafadores son muy ingeniosos: saben cómo hacer que sus declaraciones parezcan legítimas. Algunos mensajes de correo no solicitado le invitan a comprar, mientras que otros le dirigen a un sitio web con un contenido más detallado. De cualquier manera, estos consejos pueden ayudarle a evitar las estafas que llegan por el correo electrónico:

- Proteja su información personal. No proporcione la información de su tarjeta de crédito ni ninguna otra información personal a menos que esté comprando a una empresa que conozca y en la cual confíe.
- Sepa con quién está tratando. No haga negocios con ninguna empresa que no le dé su nombre, dirección física y número de teléfono.
- Tómese su tiempo. Resista la urgencia de “actuar de inmediato”, a pesar de las ofertas y los términos que se le ofrezcan. Una vez que entregue su dinero, tal vez jamás lo recupere.
- Lea la letra pequeña. Haga que todo lo que le ofrezcan se ponga por escrito y revise cuidadosamente los términos antes de realizar ningún pago o firmar cualquier contrato.
- Nunca pague por un obsequio “gratis”. Haga caso omiso de cualquier oferta que le pida que pague por un premio o un obsequio. Si algo es gratis o si es un obsequio, usted no tendría que pagar nada. Gratis es gratis.

He aquí cómo reconocer 10 estafas comunes de correo electrónico:

1. La estafa “nigeriana”

La mentira: Los estafadores se identifican como funcionarios, empresarios o la cónyuge viuda de algún funcionario importante de Nigeria o cualquier otro país y aseguran que, de alguna manera y por tiempo limitado, les es imposible el acceso a sus fondos. Le ofrecen transferirle una gran cantidad de dinero a su cuenta bancaria si usted paga una tarifa o “impuestos” para ayudarles a lograr el acceso a su dinero. Si usted responde a la oferta inicial podría recibir documentos de aspecto “oficial”. Luego le

pedirán que envíe dinero para cubrir la transacción y el costo de la transferencia y el pago de los abogados, así como una hoja en papel membretado en blanco, sus números de cuenta bancaria o cualquier otra información. Incluso podrían pedirle que viaje al país en cuestión o a un país vecino para completar la transacción. Algunos estafadores incluso presentan maletas con dinero teñido o estampado, a manera de verificación de sus declaraciones.

La realidad: Los correos son de criminales que están tratando de robarle su dinero o su identidad. Inevitablemente, en este escenario, surgen emergencias que requieren que usted envíe más dinero y que retrasan la “transferencia” de los fondos a su cuenta. Al final, usted no recibe ninguna ganancia y el estafador desaparece con su dinero.

Su red de seguridad: Si recibe un correo electrónico de alguien que asegura necesitar de su ayuda para sacar dinero de un país extranjero, no responda. Dirija cualquier estafa de este tipo, incluyendo toda la información de la dirección del correo electrónico, a spam@uce.gov. Si perdió dinero con alguno de estos trucos, llame a su oficina local del Servicio Secreto. Las oficinas locales están listadas en las Páginas Azules de su guía telefónica.

2. Phishing

La mentira: Se trata de correos electrónicos o mensajes emergentes que aseguran ser de un negocio u organización con la que tal vez usted tenga tratos, como por ejemplo, un proveedor de servicios de Internet (ISP), un banco, un servicio de pagos en línea o hasta una dependencia del gobierno. El mensaje puede pedirle que “actualice”, “valide” o “confirme” la información de su cuenta o se enfrente a terribles consecuencias.

La realidad: El Phishing es una estafa en la que los criminales utilizan Internet para enviar correos no solicitados o mensajes emergentes para reunir información personal o financiera de sus confiadas víctimas. Los mensajes le llevan a un sitio web que se ve igual al sitio de la organización legítima o le proporcionan un número de teléfono que asegura ser real. Sin embargo se trata de sitios y teléfonos falsos que sólo existen para engañarle y hacer que proporcione su información personal, de modo que los estafadores puedan robarla, pretender que son usted y gastar dinero o cometer otros delitos en su nombre.

Su red de seguridad: Como regla general, nunca responda a correos electrónicos ni mensajes emergentes que le pidan sus datos personales o financieros y le indiquen que haga clic en vínculos en el mensaje o llame por teléfono a números que aparecen en el mismo. Tampoco corte y pegue un vínculo del mensaje en la ventana de dirección de su navegador: los estafadores que

(Continúa en la página 2)



Estafas por correo electrónico (Continuación de la página 1)

utilizan la técnica del phishing pueden hacer que parezca que los vínculos van a un lugar, cuando en realidad le llevan a un sitio de aspecto similar. Si le preocupa su cuenta, póngase en contacto con la organización usando un número de teléfono que sepa que es legítimo, o inicie una nueva sesión de su navegador de Internet y escriba usted mismo la dirección Web correcta de la compañía. También puede ser de utilidad el usar programas anti-virus y anti-spyware, así como un firewall, y mantenerlos actualizados.

3. Los fraudes del trabajo en casa

La mentira: Anuncios que prometen un ingreso continuo por un trabajo mínimo (en procesamiento de reclamos de seguros médicos, relleno de sobres, trabajo de ensamblado artesanal, etc.). El anuncio utiliza frases como éstas: Dinero rápido. Trabajo mínimo. Sin riesgo alguno. Y la ventaja de trabajar desde su casa, cuando así le convenga.

La realidad: Los anuncios no dicen que tendrá que trabajar muchas horas sin sueldo ni mencionan los costos ocultos que tendrá que pagar para colocar anuncios en periódicos, sacar fotocopias o adquirir suministros, software o equipos para realizar el trabajo. Una vez que ha puesto su propio tiempo y dinero, lo más probable es que se encuentre con que los promotores se niegan a pagarle, asegurando que su trabajo no cumple con sus "estándares de calidad".

Su red de seguridad: La FTC todavía no encuentra a nadie que se haya hecho rico relleno de sobres o ensamblando imanes en su casa. Los promotores de trabajos en casa legítimos le dirán, por escrito, exactamente de lo que se trata el programa que le están vendiendo. Antes de comprometer sus recursos, averigüe qué tareas tendrá que realizar, si se le pagará un sueldo o si trabajará a comisión, quién le pagará, cuándo recibirá su primer cheque de sueldo, el costo total del programa, incluyendo suministros, equipo y cargos por membresía, y lo que obtendrá por su dinero. ¿Puede verificar la información con personas que actualmente trabajen para este negocio? Tenga presente que existen personas a las que se les paga para que mientan y que le darán muchísimas razones para que pague por el trabajo. Si lo necesita, obtenga el consejo profesional de un abogado, un contador, asesor financiero o cualquier otro experto y verifique la compañía con su agencia local de protección al consumidor, con la fiscalía del estado y con Better Business Bureau, no sólo donde se ubica la compañía, sino también en el lugar donde usted vive.

4. Los fraudes de las dietas para perder peso

La mentira: Correos electrónicos que le prometen una pastilla, parche, crema o cualquier otro producto revolucionario que le ayudará a perder peso sin hacer dieta ni ejercicio. Algunos productos aseguran bloquear la absorción de grasa, carbohidratos o calorías; otros garantizan

una pérdida de peso permanente; otros más sugieren que perderá una gran cantidad de peso a gran velocidad.

La realidad: Se trata de trucos que se aprovechan de su esperanza. No existe nada disponible por correo electrónico que usted pueda usar o aplicarse en la piel y que cause una pérdida de peso permanente o significativa.

Su red de seguridad: Los expertos aseguran que la mejor manera de perder peso es comer menos calorías e incrementar su actividad física, de manera que quemé más energía. Un objetivo razonable es perder medio kilo en una semana. En la mayoría de los casos, esto equivale a eliminar alrededor de 500 calorías de su dieta al día, comer diversos alimentos nutritivos y ejercitarse regularmente. Una pérdida de peso permanente se logra con cambios permanentes en el estilo de vida. Hable con su médico acerca de un programa de nutrición y ejercicio adecuado para su estilo de vida y metabolismo.

5. Loterías extranjeras

La mentira: Correos electrónicos en los que se anuncian magníficas probabilidades de ganar en loterías en el extranjero. ¡Incluso podrían enviarle un mensaje diciéndole que ya ganó! Sólo tiene que pagar para obtener su premio o cobrar sus ganancias.

La realidad: La mayoría de las promociones de loterías extranjeras son falsas. Los estafadores le pedirán que pague "impuestos", "derechos aduanales" o "tarifas"... y luego se quedarán con cualquier cantidad que les haya enviado. Este tipo de maleante en ocasiones le pide que le envíe los fondos a través de un giro bancario. No envíe dinero ni utilice servicios de envío de dinero o giros bancarios porque, si algo sale mal, no tendrá ningún recurso. Además, los estafadores que utilizan el engaño de la lotería usan los números de cuenta bancaria de sus víctimas para realizar retiros no autorizados o hacen cargos adicionales a sus números de tarjetas de crédito. Y un último detalle muy importante: participar en una lotería extranjera es contra la ley en Estados Unidos.

Su red de seguridad: No haga caso de estos ofrecimientos. No envíe dinero sólo porque le prometan que ganará más.

6. Productos que lo curan todo

La mentira: Correos electrónicos que aseguran que un producto es una "cura milagrosa", un "gran descubrimiento científico", un "remedio antiguo" o una cura rápida y efectiva para una amplia variedad de padecimientos y enfermedades. Por lo general anuncian una disponibilidad limitada, requieren de un pago por adelantado y le "garantizan la devolución de su dinero", en caso de insatisfacción con el producto. No es raro que cuenten con historias de casos y testimonios de consumidores o médicos que aseguran haber obtenido resultados sorprendentes.

La realidad: No existe un producto o suplemento dietético

co disponible por correo electrónico que pueda realmente reducir tumores, curar el insomnio, curar la impotencia, tratar el Alzheimer o evitar la pérdida de memoria grave. Este tipo de declaración se relaciona con formas de tratamiento de enfermedades; las compañías que quieren hacer este tipo de declaraciones deben seguir las pruebas de la FDA previas a la comercialización, así como su revisión del proceso necesario para medicamentos nuevos.

Su red de seguridad: Al evaluar declaraciones relacionadas con curas milagrosas, muéstrase escéptico. Consulte a su médico antes de comprar cualquier “cúralo-todo” que asegure tratar una amplia variedad de enfermedades o le ofrezca curas rápidas y fáciles para enfermedades graves. Por lo general, un medicamento que lo cura todo suele no curar nada.

7. Estafas con cheques con una cantidad excesiva

La mentira: Una respuesta a su anuncio o subasta en línea que le ofrece pagarle con un cheque de caja, cheque personal o cheque corporativo. En el último momento, el supuesto comprador (o el “agente” del comprador) le sale con alguna razón para hacer el cheque por más del precio de compra y le pide que le envíe la diferencia después de que deposite el cheque.

La realidad: Si deposita el cheque, usted pierde. Por lo general, se trata de cheques falsos, pero son lo bastante buenos para engañar a los cajeros del banco e incrementar temporalmente el saldo en su cuenta. Finalmente, cuando el cheque rebota, usted es responsable del pago de toda la cantidad.

Su red de seguridad: No acepte cheques por más del precio convenido de venta, sin importar lo tentador del ruego ni lo convincente de la historia. Pida al comprador que haga el cheque por el precio de la compra. Si el comprador le envía un cheque con la cantidad incorrecta, devuélvalo. No envíe la mercancía. Como vendedor que acepta pagos con cheque, podría solicitar un cheque de un banco local o un banco con una sucursal local. De esa manera puede visitar personalmente el banco y asegurarse de que el cheque sea válido. Si no es posible, llame al banco que otorgó los cheques usando el número de teléfono en la guía telefónica o en un sitio de Internet que conozca y en el que confíe. No obtenga el número de la persona que le proporcione el cheque. Pregunte si el cheque es válido.

Informe de cualquier estafa de pago excesivo con cheque a spam@uce.gov y al fiscal general de su estado. Puede encontrar la información de contacto del fiscal general de su estado en www.naag.org.

8. Ofertas de crédito que debe pagarse por anticipado

La mentira: Le informan que ha “pre-calificado” para

obtener un préstamo o tarjeta de crédito con un interés bajo, o para arreglar un mal historial de crédito, incluso si los bancos le han rechazado. Pero para aprovechar esta oferta, usted tiene que pagar un cargo de procesamiento de varios cientos de dólares.

La realidad: Una oferta legítima de pre-calificación significa que se le ha seleccionado para que pida un crédito. Todavía tiene que completar el proceso de solicitud y puede rechazársele. Si ha tenido que pagar una tarifa por adelantado, con la promesa de recibir un préstamo o crédito, lo han estafado. Es posible que reciba una lista de prestamista, pero no un crédito, y la persona a la que le haya pagado se quedará con su dinero y desaparecerá.

Su red de seguridad: No pague por promesas. Los prestamistas legítimos nunca “garantizan” una tarjeta o préstamo antes de que usted lo solicite. Tal vez le pidan que pague una tarifa por la solicitud, la evaluación o el informe de crédito, pero este dinero rara vez se pide antes de que se identifique a la institución que otorgará el crédito y de que se complete la solicitud. Además, los cargos por lo general se pagan al prestamista y no al intermediario o a la persona que haya arreglado el préstamo “garantizado”.

9. Falsa ayuda para salir de deudas

La mentira: Correos electrónicos que le aseguran contar con una manera en la que podrá consolidar sus deudas en un solo pago mensual, sin tener que recurrir a préstamos, ayuda para poner un alto a los cobradores, ejecuciones hipotecarias, reposiciones, cobros de impuestos y confiscaciones legales o la eliminación total de sus deudas.

La realidad: Estas ofertas con frecuencia involucran procedimientos de bancarrota, pero rara vez lo dicen. Aunque declararse en bancarrota es una manera de hacer frente a problemas financieros serios, por lo general se considera como el último recurso. La razón: tiene un impacto negativo de largo plazo sobre su capacidad crediticia. Una declaración de bancarrota permanece en su historial crediticio durante 10 años y puede afectar su habilidad para obtener un crédito, un trabajo, un seguro y hasta un sitio donde vivir. Encima de todo, lo más probable es que tenga que pagar los honorarios del abogado que le lleve el proceso para declararse en bancarrota.

Su red de seguridad: Lea entre líneas cuando reciba este tipo de correo electrónico. Antes de recurrir a la bancarrota, hable con sus acreedores acerca de la forma en que puede establecerse un plan de pagos modificado, hable con un servicio de asesoría crediticia para que le ayude a desarrollar un plan para el pago de sus deudas o considere cuidadosamente obtener una segunda hipoteca o una línea de crédito basada en la plusvalía de su hogar. Una advertencia: Un préstamo sobre su casa podría ayudarle a consolidar sus deudas, pero también requiere que ponga su casa como garantía. Si no puede realizar los pagos, podría perder su hogar.

10. Inversiones fraudulentas

La mentira: Correos electrónicos que le ofrecen "inversiones" que le prometen grandes ganancias con muy poco riesgo. Una versión busca inversionistas para ayudar a formar un banco en el extranjero. Otras son vagas acerca de la naturaleza de la inversión, pero subrayan las excelentes ganancias. Los promotores presumen de magníficas conexiones en los altos círculos financieros, del hecho de que cuentan con información interna, de que garantizan la inversión o le comprarán las acciones cuando usted quiera salir del negocio. Para cerrar el trato, con frecuencia utilizan estadísticas falsas, interpretan en su favor la importancia de un suceso actual o hacen énfasis en la calidad única de la oferta. Casi siempre tratan de apresurarlo para tomar una decisión.

La realidad: Muchos de estos negocios son excelentes para los promotores, pero no para los participantes. Los promotores de inversiones fraudulentas operan este tipo particular de estafa durante un corto tiempo, y desaparecen antes de que las autoridades puedan detectarlos, gastando con rapidez el dinero que obtienen. Con frecuencia, vuelven a las andadas con otro nombre, vendiendo algún otro tipo de estafa de inversiones.

Su red de seguridad: Tómese su tiempo para evaluar la legitimidad de la oferta: cuanto mayor sea la ganancia que se le prometa, mayor será el riesgo. No deje que lo presionen a comprometerse a realizar una inversión antes de estar seguro de que es legítima. Además, contrate a un abogado o a un contador para que revise cualquier oferta de inversión.

Defiéndase

Si recibe un correo electrónico que usted considere que podría ser una estafa, envíelo a la FTC al spam@uce.gov y al escritorio de abusos del remitente de su proveedor de servicios de Internet. Además, si el mensaje parece estar suplantando a un banco o a cualquier otra empresa u organización, reenvíeles el mensaje. Los estafadores son inteligentes y astutos y constantemente encuentran nuevas variaciones de viejos timos. Con todo, los consumidores escépticos pueden identificar promociones cuestionables o de dudosa legitimidad en los ofrecimientos que reciben por correo electrónico. Si recibe un mensaje que cree que pueda ser fraudulento, reenvíelo a la FTC, bórralo de su correo y sonría. Estará haciendo su parte para ayudar a llevar a un estafador ante la justicia.

<http://www.onguardonline.gov/>

OnGuardOnline.gov le ofrece consejos prácticos por parte del gobierno federal y de la industria de la tecnología para ayudarle a mantenerse en guardia en contra del fraude por Internet, asegurar su computadora y proteger su información personal.

¿Está tenso y abrumado? ¿Se enfurece con facilidad? Llame al Programa de asistencia a empleados y a miembros (EAP/MAP) y reciba ayuda gratuita y confidencial. 1-800-292-2780