Ciberseguridad y seguridad en internet

Manual y guía de recursos del Proyecto Piers (versión 2019)

Una iniciativa del Front Porch Center for Innovation and Wellbeing

Patrocinado adicionalmente por

California Lutheran Homes

Front Porch, una organización no lucrativa de servicios humanos que promueve comunidades innovadoras y programas que satisfacen las necesidades cambiantes de las personas conforme envejecen, ha recibido una generosa donación monetaria a nombre de la familia de una de las antiguas residentes de una comunidad de jubilados, Ellie Piers.

Ellie Piers

La donación beneficia la misión continua del Front Porch Center for Innovation and Wellbeing (FPCIW) de usar la tecnología para mejorar el bienestar entre los adultos mayores. Piers vivía en Carlsbad By The Sea, una comunidad de jubilados de Front Porch en Carlsbad, CA. Su contribución permitió al CIW (Center for Innovation and Wellbeing) abordar el problema de la seguridad de los adultos mayores por medio de la tecnología de la información para desarrollar iniciativas relacionadas con la seguridad en línea de los adultos mayores en el área metropolitana de San Diego. Así mismo, facilitar que estas iniciativas también sean accesibles a comunidades lejanas en todo el internet.

Piers tenía una mente curiosa y un espíritu aventurero en cuanto a la tecnología y creía que esta podía ayudar a los adultos mayores a vivir bien y de forma segura. Aceptó la oportunidad de acercarse a la tecnología para mantenerse en contacto con amigos y familiares, pero siempre teniendo en mente los problemas de seguridad que acompañan al uso de la tecnología. Piers contaba con un buen sentido de la vulnerabilidad que surge con el uso de la tecnología y tenía el hábito de hacer preguntas concienzudas antes de aventurarse en la red y esto le ayudaba en sus episodios de "navegación en internet". Al celebrar el espíritu de Piers mediante la ayuda hacia otros, el FPCIW ha desarrollado el **Proyecto Piers** para abordar la seguridad de los adultos mayores y crear conciencia mediante:

- La puesta a prueba de tecnologías emergentes relacionadas con la seguridad de los adultos mayores y el desarrollo de contenido relacionado con la seguridad en línea para adultos mayores;
- El establecimiento de conexiones con organizaciones en el área metropolitana de San Diego que tienen conocimientos en esa área para establecer una colaboración que maximice las contribuciones y crear un mayor impacto en el problema de la seguridad en línea de los adultos mayores;
- La exploración de medios para crear conciencia sobre la tecnología que pueda mejorar la vida de los adultos mayores en el área metropolitana de San Diego; y
- La creación de una campaña en línea y en las redes sociales que rinda tributo a la donación de Piers y su interés en marcar la diferencia en esta importante área del bienestar de los adultos mayores.

Este manual, creado por el FPCIW, también ha sido patrocinado por California Lutheran Homes Foundation para hacer llegar este recurso a más comunidades en más idiomas. Nuestro manual es una guía para que las personas entiendan mejor algunos de los riesgos del mundo en línea y para ayudar a que se puedan evitar de forma proactiva y confiada cuando se disfruten los beneficios del internet.

Manual de Ciberseguridad

Índice

¿Sabía usted que...?

- En 2016, el **67% de estadounidenses** de 65 años o más usaban el internet[1].
- Únicamente se denuncia **1 de cada 24 casos de abuso de ancianos**[2].
- En 2017, los adultos mayores perdieron **$1,700 millones por abuso financiero**[3].
- **El 45% del abuso financiero** comienza mediante el uso del internet[4].
- **El 59% de las personas** dice que no están seguros de si lo que ven en los medios es cierto[5].

Hoy en día la tecnología se ha vuelto una herramienta integral en nuestra vida cotidiana. Hablamos con nuestros seres querido por internet, hacemos nuestras operaciones bancarias y compras en línea, socializamos en plataformas como Facebook y Twitter, e investigamos nuestros temas favoritos. El internet tiene muchos beneficios, pero ¿cómo aprovechar este inmenso universo digital de forma segura?

Como miembros activos de una sociedad digital, es importante que tengamos buenos hábitos de internet. Debemos estar alertas a las tácticas indebidas que algunas personas usan para aprovecharse de nuestra información personal y ocasionar daño personal, social o financiero. Como cualquier aptitud útil, es importante tomar medidas preventivas que puedan reducir los riesgos y nos permitan utilizar los beneficios del internet con tranquilidad, seguridad y confianza. Nuestro poder y control provienen del conocimiento y de las experiencias compartidas.

Este manual está diseñado para ser una guía de recursos sobre el uso seguro de las computadoras para los adultos mayores. Las lecciones en este manual se basan en tres reglas simples, pero importantes sobre las experiencias seguras y positivas en línea.

1) **CUESTIONE** el contenido que ve en internet ,
2) **VERIFIQUE** su validez y autenticidad, y
3) **PREGUNTE** a sus amigos, vecinos o colegas si necesita ayuda y para informar a las personas a su alrededor.

Ciberseguridad y adultos mayores como blanco principal

La ciberseguridad se refiere a la seguridad en internet en general y en particular se refiere a la protección de información que se almacena en computadoras o que es accesible por medio del internet. El fraude que usa varias formas de tecnología, incluyendo las computadoras y el internet está experimentando un avance continuo.

Cualquier persona que use el internet puede ser blanco de los cibercriminales, pero ¿por qué el blanco más común son los adultos mayores? Los adultos mayores tienen más probabilidades de tener cierta seguridad financiera, es menos probable que denuncien un fraude o tal vez no sepan adónde acudir para denunciar un incidente así. Los adultos mayores también podrían invertir grandes cantidades de fondos en productos que prometen falsamente mejorar la memoria, la longevidad o la salud física.

Los adultos mayores tienden a no denunciar los crímenes por miedo o vergüenza, lo cual perpetúa el abuso financiero de más víctimas [9]. Si ha sido víctima de un cibercrimen anteriormente, tal vez le ayude saber que **no es el único** y que muchas personas se han enfrentado a los mismos retos.

Es vital que toda la población que no esté familiarizada con el uso de la tecnología de consumo aprenda técnicas para evitar activamente el ciberfraude. El objetivo del manual del Proyecto Piers es prevenir el maltrato en línea de los adultos mayores y darles las armas que les permitan beneficiarse de la tecnología de la información, por medio del comportamiento seguro en línea.

¿A quién creer? ¡Identifique al impostor!

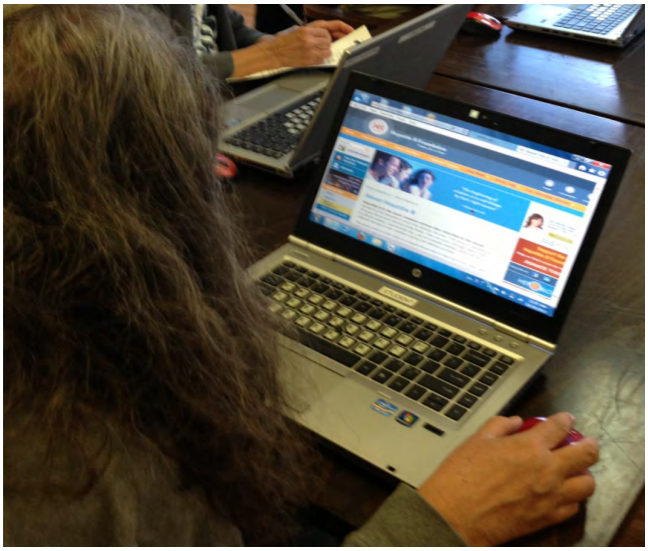
Uno de los múltiples beneficios del internet es la comodidad de manejar muchos aspectos de nuestra vida, ya sea algo relacionado con la salud, los impuestos o las finanzas. Fácilmente podemos encontrar la información necesaria y conectarnos con las personas correctas en caso de requerir ayuda. Cuando usamos el internet, es importante poder identificar y distinguir a los estafadores e impostores.

El robo de identidad ocurre cuando una persona obtiene o usa su información de identificación personal sin su autorización o consentimiento. Esta información puede usarse para comprar artículos, recibir beneficios de Seguridad Social, robar sus finanzas personales o cometer otros crímenes. Ser víctima del robo de identidad puede resultar en consecuencias graves. Algunos ejemplos incluyen un pasaporte copiado ilegalmente, depreciación de su crédito o fraude de Medicare o Medicaid. A continuación le presentamos una lista de las estafas más comunes a las que hay que estar alerta y qué puede hacer para tomar acciones preventivas y proceder con seguridad:

Estafas relacionadas con el cuidado de la salud. Este tipo de estafas ocurren de diferentes formas, incluyendo comerciales de televisión falsos, que se aprovechan de requisitos legales nuevos, que conciernen a quienes reciban tarjetas de salud adicionales, o pueden ser llamadas telefónicas que prometen grandes descuentos en seguros de salud.

1) **CUESTIONE** el contenido que ve en el internet,
2) **VERIFIQUE** su validez y autenticidad, y
3) **PREGUNTE** a sus amigos, vecinos o colegas si necesita ayuda y para informar a las personas a su alrededor.

Otras estafas consisten de fraude de suplantación, en el que alguien pretende ser un funcionario del gobierno que necesita su número de Medicare para poder enviarle una tarjeta de beneficiario actualizada.



¡Esto es lo que puede hacer!

- ✓ **Manténgase al día en cuanto a los acontecimientos actuales**. Los estafadores con frecuencia planean realizar sus ataques en los periodos en que Medicare y otros planes de salud sufren cambios que se abordan en los medios ampliamente[6]. Esté preparado y sea cauteloso durante la temporada de inscripción a Medicare. Como parte de la Iniciativa de Eliminación del Número de Seguridad Social (SSNRI, por sus siglas en inglés), a partir de abril de 2018, los Centros de Servicio de Medicare y Medicaid han comenzado a expedir y enviar nuevas tarjetas de Medicare para reemplazar las tarjetas antiguas que contenían el número de Seguridad Social.
- ✓ **Investigue para confirmar si lo que dicen es verdad**. Antes de compartir su información privada, contacte a Medicare (1-800-MEDICARE) para estar seguro. Debe saber que Medicare nunca le llamará, así que si recibe una llamada no dé ninguna información personal.

Fraude fiscal. Las estafas de phishing con el formulario W-2 recientemente se han vuelto una inquietud importante en la ciberseguridad. Los estafadores han encontrado formas de enviar emails (mensajes de correo electrónico) falsos que parecen proceder de un director empresarial u otros ejecutivos solicitando la información del formulario W-2 de sus empleados. Los cibercriminales usan la información del W-2 y presentan declaraciones de impuestos falsas y roban la identidad de las personas[7].

¡Esto es lo que puede hacer!

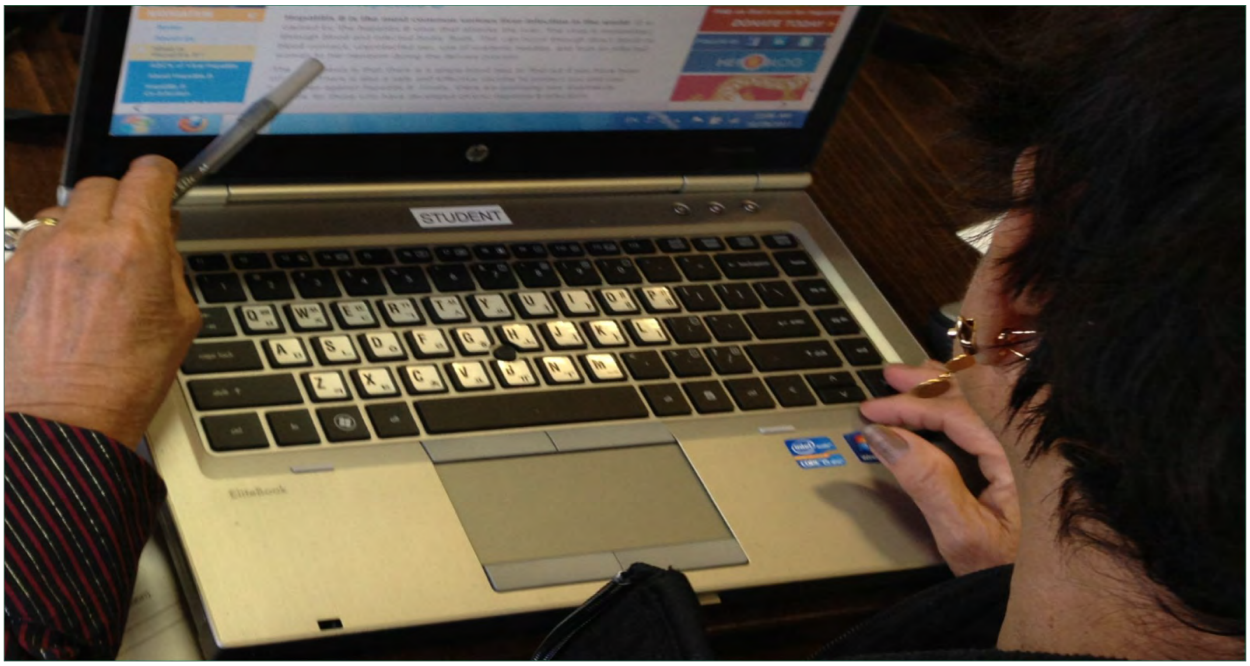
- ✓ **Haga una llamada**. Si recibe un email solicitando su información fiscal del formulario W-2, llame a su compañía para verificar esta petición antes de enviar cualquier información.
- ✓ **Declare sus impuestos con anticipación**. Al declarar sus impuestos lo antes posible, puede adelantarse a los cibercriminales antes de que ellos presenten una declaración fraudulenta.
- ✓ **Verifique su informe crediticio regularmente.** Puede revisar su crédito de forma gratuita una vez al año en AnnualCreditReport.com y congelar cualquier cuenta en la que haya alguna actividad sospechosa.

Fraude de lotería. Este tipo de actividad ilegal incluye declaraciones falsas de que usted ha sido elegido como ganador de una lotería, además de pedirle el pago de cuotas iniciales. El fraude de lotería por email usa nombres de organizaciones de lotería u otras corporaciones legítimas. Tómelo con calma, investigue y si es demasiado bueno para ser realidad, probablemente lo sea.

Fraude de inversiones. Estas peticiones son respecto a inversiones en fondos nuevos o existentes. Es posible que le pidan que invierta en cualquier cosa, desde minas, petróleo, gas o una nueva compañía de tecnología. Un ejemplo típico es "Prime Bank". Los promotores aseguran que los fondos de los inversionistas se usarán para comprar y comerciar un instrumento "Prime Bank", emitido o garantizado por una organización oficial como la Reserva Federal de los Estados Unidos. También con frecuencia suelen decir que las oportunidades de inversión de este tipo solo están disponibles mediante una invitación exclusiva para un selecto grupo de clientes[8]. Además las inversiones fuera del país deben ser examinadas cuidadosamente y requieren una mayor cautela, como resultado de los reglamentos y controles nacionales.

¡Esto es lo que puede hacer!

- ✓ **Las apariencias engañan.** Algunos sitios web pueden tener una apariencia atractiva y legítima, pero eso no siempre significa que sean confiables.
- ✓ **Pregunte sobre el acuerdo de condiciones y términos.** Se le aconseja que revise cuidadosamente este acuerdo, pues las personas frecuentemente ignoran detalles importantes.
- ✓ **No crea en las promesas de grandes cantidades de dinero.** Esta es una táctica común que se usa como anzuelo por email.



Emails o mensajes de correo electrónico

Los emails son un modo de comunicación fundamental en internet, pero ¿cómo saber cuáles son seguros de abrir y cuáles debe eliminar? ¿Cuáles son algunas pistas a las que debe poner atención? A continuación verá algunos términos que debe conocer y lo que puede hacer para reconocer las posibles amenazas en su bandeja de entrada.

Phishing o suplantación de identidad. Cuando un estafador usa emails o mensajes de texto fraudulentos para lograr que usted comparta información valiosa, se le llama "phishing". Al igual que "fishing" (que significa "pescar"), los estafadores tratan que la víctima muerda el anzuelo con un enlace o sitio web falso que aparenta ser legítimo y seguro. Esa es la forma en que recopilan contraseñas, números de seguridad social, información de cuentas bancarias, etc.

Spam o correo basura. Se trata de emails no solicitados y masivos que pueden usarse para cometer una gran diversidad de fraudes en línea. La mayoría del spam es inofensivo, y se trata de mensajes molestos de publicidad, pero algunos pueden tener acceso a computadoras y servidores sin autorización y transmitir virus. Esta forma de fraude también puede obtener y vender ilegalmente su información privada.

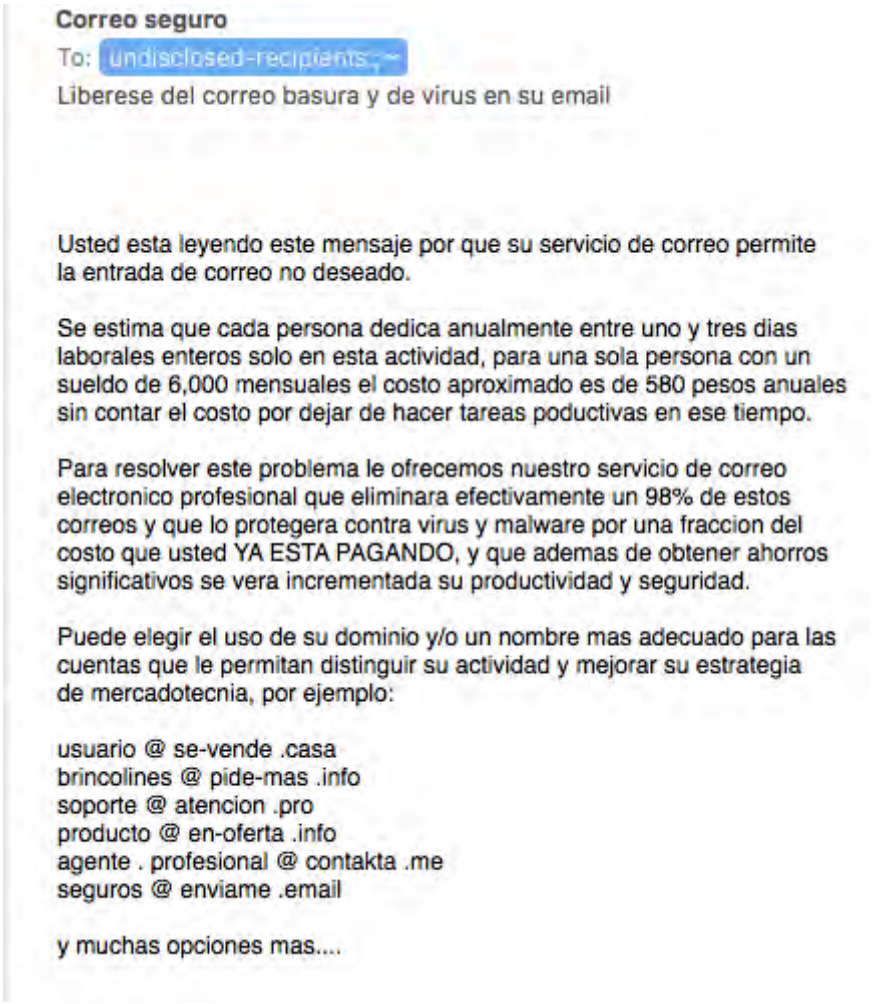
Hacking o piratería informática. Una persona que logra tener acceso a sus computadoras de forma remota o a sus cuentas personales sin autorización es un hacker. Cualquier forma de hacking que se aproveche de las debilidades de un sistema informático o una red informática se considera una actividad ilegal y criminal.

Fraude de la carta de Nigeria/Fraude 419. Esta estafa, también conocida como Fraude de pago por adelantado, solicita su información personal o bancaria por email, alegando que el remitente es un funcionario gubernamental de un país extranjero o un extranjero que necesita ayuda financiera. Este mensaje anima al destinatario a enviar información al autor, tal como papelería membretada en blanco, con el nombre de su banco y número de cuenta y otro tipo de información privada a la que puedan acceder también por medio de un número de fax (que se proporciona en la carta)[9]. Sea escéptico de los mensajes de gobiernos extranjeros. Generalmente solicitan ayuda solicitando un depósito considerable a un banco ubicado fuera de su país. Este tipo de estafadores generalmente hacen un llamado urgente y solicitan su ayuda financiera. También desconfíe de los emails del gobierno de Estados Unidos y tenga cuidado con los mensajes que vienen de alguien que asegura provenir de la Administración de Seguro Social donde le piden su número de seguro social. ¡Piénselo dos veces! Normalmente este tipo de organizaciones no le solicitarían su información personal por medio del internet.

Analicemos más de cerca

Las estafas de phishing no se limitan solamente a fuentes de Nigeria. Desconfíe de cualquier email que pida ayuda para transferir grandes cantidades de dinero, incluyendo las que parecen provenir de un amigo o familiar en un caso de emergencia cuestionable.

Siempre VERIFIQUE la validez y llame a un familiar mutuo o a un amigo para confirmar.



Correo seguro

To: undisclosed-recipients;

Liberese del correo basura y de virus en su email

Usted esta leyendo este mensaje por que su servicio de correo permite la entrada de correo no deseado.

Se estima que cada persona dedica anualmente entre uno y tres dias laborales enteros solo en esta actividad, para una sola persona con un sueldo de 6,000 mensuales el costo aproximado es de 580 pesos anuales sin contar el costo por dejar de hacer tareas poductivas en ese tiempo.

Para resolver este problema le ofrecemos nuestro servicio de correo electronico profesional que eliminara efectivamente un 98% de estos correos y que lo protegera contra virus y malware por una fraccion del costo que usted YA ESTA PAGANDO, y que ademas de obtener ahorros significativos se vera incrementada su productividad y seguridad.

Puede elegir el uso de su dominio y/o un nombre mas adecuado para las cuentas que le permitan distinguir su actividad y mejorar su estrategia de mercadotecnia, por ejemplo:

usuario @ se-vende .casa
brincolines @ pide-mas .info
soporte @ atencion .pro
producto @ en-oferta .info
agente . profesional @ contakta .me
seguros @ enviame .email

y muchas opciones mas....

¡Esto es lo que puede hacer!

- ✓ **Ponga atención a la ortografía y gramática del email**. Revise la ortografía de las URLs, la dirección de email y el contenido del mensaje. Los emails de phishing comúnmente tienen errores sutiles de ortografía que puede identificar. Cuando vea el nombre del remitente, dé otro vistazo para revisar la dirección de email de donde viene el mensaje. Además si mantiene el puntero del ratón sobre los enlaces, podría ver que lo llevarán a un sitio sospechoso en lugar del sitio web al que promete enlazarlo.
- ✓ **No abra los emails de una fuente desconocida.** Si le llega un email, mensaje de texto o de redes sociales de una persona desconocida, bórrelo o ignórelo. Use la misma cautela con los emails que indican que debe reclamar dinero, regalos o una oferta de vacaciones. Lo más probable es que el mensaje lo envíe a otro sitio web desde donde pueda recibir malware o virus. Si no está seguro ¡elimínelo!
- ✓ **Sospeche de los enlaces en emails o mensajes de texto**. Si recibe un email de alguien conocido, pero el único contenido del email es un enlace, no haga clic en el enlace. Esta es una señal común de que la persona que envió el email podría haber sido hackeada. En una situación como esta, contacte a la persona por teléfono u otro medio y borre el email.
- ✓ **Nunca dé su número de cuenta bancaria o información personal por email**. Sepa que las compañías legítimas como bancos y compañías de seguro jamás le pedirán su información personal por email. En su lugar acuda al sitio web seguro y entre a su cuenta para ver mensajes o notificaciones.

1) **CUESTIONE** el contenido que ve en el internet,
2) **VERIFIQUE** su validez y autenticidad, y
3) **PREGUNTE** a sus amigos, vecinos o colegas si necesita ayuda y para informar a las personas a su alrededor.

Analicemos más de cerca

Los estafadores a menudo usan nombres de compañías conocidas en sus emails para que usted crea que puede confiar y hacer clic en el enlace incluido. Dé un vistazo al email a continuación. Este es un ejemplo real de un email "phishing" que la policía denunció en Ohio en diciembre de 2018 y *aparenta* provenir de Netflix.

Si duda sobre si es seguro hacer clic en un enlace en un email de una compañía, lo más seguro es abrir una nueva ventana del navegador, ir directamente al sitio web de la compañía y entrar a su cuenta. Si hay alguna notificación o mensaje importante respecto a su cuenta, generalmente estarán ahí dentro de su cuenta en el sitio web seguro.

Cómo proteger sus finanzas

Hay muchos beneficios de usar el internet para manejar sus finanzas: hacer compras prácticas en línea, programar y pagar sus cuentas o transferir fondos de forma instantánea. El fraude financiero en línea viene en distintas formas, y el tipo más común de fraude involucra el uso de tarjetas de crédito o la información bancaria, que generalmente se usan para realizar compras, inversiones o provocar alguna complicación fiscal. La información necesaria para este tipo de estafa se puede obtener por medio de sitios web o emails fraudulentos.

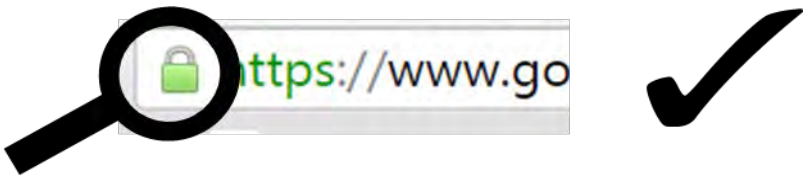
Compras en línea. La actividad fraudulenta podría incluir el uso de una tarjeta de débito o crédito. Esto se puede lograr por medio del robo de la tarjeta real o al obtener ilegalmente la información personal y de la cuenta del titular de la tarjeta, incluyendo el número de la tarjeta, el código de seguridad, el nombre del titular y su domicilio.

¡Esto es lo que puede hacer!

- ✓ **Use métodos de pago alternativos siempre que pueda.** En lugar de hacer un pago directamente en un sitio web, use servicios alternativos de pago tales como PayPal, Amazon y Google Check Out, los cuales usan niveles adicionales de seguridad[10]. Siempre que pueda también haga su pago como "visitante" y elija no guardar la información de su tarjeta en una cuenta.
- ✓ **Ponga atención a su estado de cuenta**. Tenga una lista organizada de sus tarjetas de crédito activas y revise sus estados de cuenta regularmente. Contacte a su emisor de tarjeta de crédito de inmediato si nota cualquier cosa errónea o desconocida.
- ✓ **Use tarjetas de crédito cuando pueda.** Generalmente es más seguro usar tarjetas de crédito y no de débito porque le permiten al comprador pedir el crédito al emisor en caso de que no reciba el producto que ordenó[11].
- ✓ **Habilite las herramientas de autenticación más potentes.** Puede proteger sus cuentas de compras en línea al habilitar las herramientas de autenticación más potentes tales como biometría, claves de seguridad o un código único de un solo uso por medio de una aplicación en su dispositivo móvil[11].

Analicemos más de cerca

Busque el símbolo del candado. Cuando uno entra a un sitio web y aparece un pequeño candado en la barra de la dirección de internet, esto indica que ese sitio web usa un nivel de seguridad *más elevado* para transmitir datos. Aunque este ícono representa la utilización de cierta protección, ¡no garantiza necesariamente que sea un sitio completamente seguro!



Revise la dirección del enlace. Los enlaces que parecen legítimos externamente podrían no ser auténticos, así que léalo cuidadosamente. Por ejemplo, el enlace podría decir “bankofamericacard.com” o “B-of-America”— incluyendo la palabra “bank” o “America”, que da la apariencia de ser legítimo, pero no es un enlace al sitio web verdadero de la compañía.

Visite el sitio web de la Comisión Federal de Comercio **www.ftc.gov** para más consejos y ayuda al consumidor en línea.

Actividad bancaria en línea. Cuando se conecta de forma segura al sitio web o a la aplicación de su banco, puede hacer sus operaciones bancarias en línea con toda confianza. Busque las mismas señales de seguridad a las que debe estar atento cuando haga compras en línea (el candado verde, "https" y la ortografía correcta de la URL). A continuación encontrará más consejos para estar seguro en línea al realizar operaciones bancarias.

¡Esto es lo que puede hacer!

- ✓ **Use su conexión de Wi-Fi personal para realizar sus operaciones bancarias en línea**. No use Wi-fi gratuito o público para hacer cualquier actividad que requiera información delicada.
- ✓ **Revise sus estados de cuenta regularmente**. Asegúrese de que todas las compras que vea sean conocidas. Si nota cualquier actividad sospechosa en su cuenta, contacte a su banco de inmediato.
- ✓ **Antes de dejar el sitio web o aplicación de su banco, asegúrese de cerrar su sesión.** Incluso podría cerrar su navegador por completo después de cerrar la sesión.
- ✓ **Pregunte sobre la póliza de seguro de su banco**. En caso de que un cibercriminal logre obtener su información bancaria, es bueno saber con anticipación cuáles son las políticas y procedimientos de su banco para reembolsarle en caso de que ocurra alguna actividad fraudulenta. ¿Cuánto tiempo tiene para presentar un reclamo y cuánto cubrirá su banco?

1) **CUESTIONE** el contenido que ve en el internet,
2) **VERIFIQUE** su validez y autenticidad, y
3) **PREGUNTE** a sus amigos, vecinos o colegas si necesita ayuda y para informar a las personas a su alrededor.

Malware o software malicioso

¿Cómo saber dónde es seguro hacer clic y dónde no lo es? Queremos poder recibir mensajes que genuinamente están dirigidos a nosotros y que provienen de fuentes confiables, así que estas son algunas cosas importantes que debe saber.

Clickbait o ciberanzuelo se refiere al contenido en internet cuyo propósito es llamar la atención y captar visitantes a un enlace de una página web en particular. Algunos encabezados o anuncios podrían realmente llevarlo a un artículo interesante o a una tienda en línea que le gustaría visitar. Sin embargo, sitios que usan muchos encabezados como ciberanzuelo tienen más probabilidades de contener malware.

Malware. Malware es la versión corta de "software malicioso", está diseñado para causar daño o crear problemas en un sistema informático. Es importante también ser cuidadoso con su dispositivo móvil, pues no son inmunes a los ataques de malware y virus. De acuerdo con wikipedia.org, "El malware puede ser sigiloso y busca robar información o espiar a los usuarios de computadoras durante periodos prolongados sin que estos se enteren". El malware tiene varias categorías de software:

Ransomware o secuestro de datos. Una combinación de los términos en inglés '*ransom*' (rescate) y '*software*' (programa). El ransomware se refiere a cualquier malware que puede congelar su computadora a distancia y retirar información almacenada o incluso solicitarle compensación financiera para regresar los fondos robados. Las personas que distribuyen este malware se identifican falsamente como una figura de autoridad, tal como la policía. Estos ataques dañinos de ransomware también pueden estar dirigidos a teléfonos inteligentes o tabletas.

Virus. Los virus que atacan a las personas son similares a los virus de las computadoras. Hablando en términos tecnológicos usan a las computadoras como huésped para su propia sobrevivencia. Al hacer esto, los virus pueden seguir multiplicándose y modificándose dentro de su computadora para lograr su misión, diseminar más malware a otros durante el ataque.

Programas vacuna. Las vacunas, también conocidas como "software anti-virus" funcionan como una medida preventiva o de contraataque en contra del malware. Confirme que su computadora tiene al menos un programa de antivirus activo (o un Firewall de Windows) para prevenir ataques de malware. Estos programas pueden ser especialmente necesarios si su computadora recientemente experimenta una reducción en su velocidad de procesamiento.

Hay muchos programas vacuna disponibles con diversas opciones de funciones y precios. Algunas marcas comunes son:

- Avast
- AVG
- Bitdefender Antivirus
- Kaspersky Anti-Virus
- McAfee AntiVirus
- Norton Security

Programa anti-malware. Las funciones de Firewall de Windows son la forma más básica de protección contra malware y están integradas en el programa Microsoft Windows. Sin embargo para los usuarios de Apple Mac es importante confirmar que las actualizaciones de software están habilitadas en el menú Apple. Además, los usuarios de Apple deben permitir los chequeos de actualizaciones programados en la opción de "Preferencias del sistema". Las extensiones del navegador como uBlock Origin pueden bloquear anuncios o publicidad que rastrean su actividad e instalan malware.

Analicemos más de cerca

Estas son algunas señales de alerta a las que debe estar atento en su computadora:

- La computadora se congela o funciona más lentamente
- Sonidos inusuales o pitidos
- Notificaciones en ventanas emergentes
- Imágenes no deseadas
- Datos que desaparecen

Regularmente averigüe si hay actualizaciones de su antivirus y haga un escaneo completo como confirmación[12]. No olvide renovar su suscripción anual para mantener su software actualizado en contra de nuevos ataques.

¡Esto es lo que puede hacer!

- ✓ **Ciérrelo**. Si un anuncio de ventana emergente o un sitio web se ven sospechosos, simplemente ciérrelo haciendo clic en la casilla de la esquina superior derecha con la "X". Si su navegador o programa antivirus cuestiona la seguridad de un sitio web, no lo visite [11].
- ✓ **No descargue** nada a menos que sea completamente consciente de lo que es y de que proviene de una fuente segura.
- ✓ **Los anuncios y ventanas emergentes** con frecuencia pueden parecerse a una advertencia de diagnóstico del sistema o pueden indicar que usted ha ganado un premio. No haga clic en estas ventanas. Ciérrelas de inmediato y ejecute un escaneo normal de antivirus en su computadora o dispositivo. A continuación hay algunos ejemplos de ventanas emergentes comunes que debe evitar.

Seguridad de contraseñas

Debemos tartar nuestra información personal como si fuera dinero. *Debemos valorarla y protegerla.* La seguridad de las contraseñas es crucial porque dan acceso a la información personal valiosa. Piense que la contraseña es como las llaves de su casa. Un aspecto importante para protegernos es crear contraseñas que sean difíciles de adivinar para los demás.

<u>Cómo crear una contraseña fuerte.</u>

- ✓ Que sea larga. Es ideal que sean más de 6 caracteres.
- ✓ No usen la misma contraseña para todas sus cuentas.
- ✓ Usen una mezcla de letras, números y símbolos.
- ✓ No usen información personal como el nombre de sus hijos, fecha de nacimiento, edad o domicilio.
- ✓ Cambien su contraseña regularmente. Los expertos recomiendan que lo hagan por lo menos cada 6 meses.

<u>Manejo de contraseñas.</u> Los programas de manejo de contraseñas le ayudan a usar una contraseña para varias cuentas. Llenan automáticamente su información de cuenta para los sitios webs que usted haya registrado. Tome en cuenta investigar los pros y contras de cada programa para averiguar cuál es el mejor para usted. Algunos ejemplos de programas gratuitos con servicios de paga opcionales son:

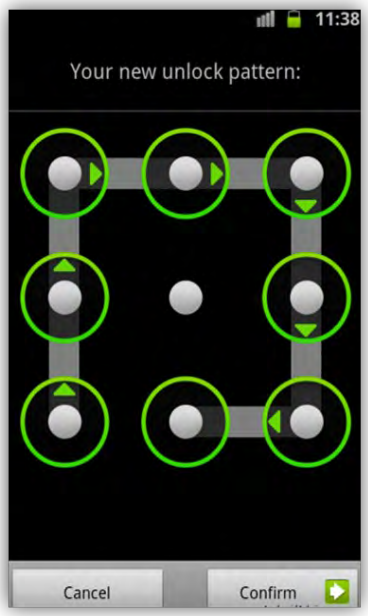
- LastPass
- Keeper
- Dashlane

¿Su contraseña está en esta lista?

Los hackers entran a nuestras cuentas al adivinar nuestra contraseña, así que no permita que sea fácil para ellos descifrarla. Asegúrese de no usar ninguna de las contraseñas a continuación. Estas son las 25 contraseñas usadas más comúnmente y por lo tanto son fáciles de hackear – contraseñas de 2018*

RANK	PASSWORD
1	123456
2	password
3	123456789
4	12345678
5	12345
6	111111
7	1234567
8	sunshine
9	qwerty
10	iloveyou
11	princess
12	admin
13	welcome
14	666666
15	abc123
16	football
17	123123
18	monkey
19	654321
20	!@#$%^&*
21	charlie
22	aa123456
23	donald
24	password1
25	qwerty123

**SplashData, 2018*



Asegúrese de bloquear sus dispositivos, ya sea una computadora de escritorio, portátil, tableta o teléfono inteligente. Su dispositivo le permite establecer una contraseña para que solo usted pueda usarlo.

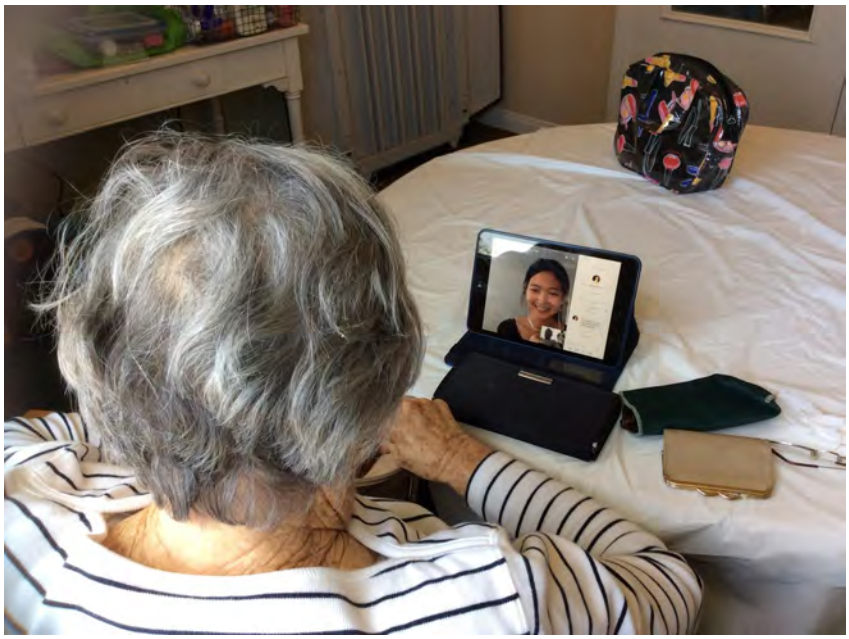
Autenticación de dos factores. Al permitir la autenticación de dos factores (2FA, por sus siglas en inglés) agrega un nivel adicional de seguridad para desalentar a las personas que intenten acceder a su cuenta. Esto significa que aún si alguien averiguara su contraseña, necesitan tener acceso físico a su teléfono para poder acceder a su cuenta. Esto es lo que significa que sean dos factores: algo que usted sabe (su contraseña) y algo que usted posee (su teléfono celular)[13]. Las herramientas de autenticación pueden ser en forma de biometría, claves de seguridad o un código único que usará solo una vez mediante una aplicación en su dispositivo móvil[14].

Asistentes inteligentes, hogares inteligentes y Wi-Fi

Conforme se vuelven más comunes en el hogar los asistentes de voz como Alexa de Amazon, es importante ser conscientes de las medidas de seguridad que podemos tomar para proteger nuestra privacidad. El **IoT** (que en inglés significa "Internet de los objetos") se refiere a la capacidad de conexión a redes que permite que objetos y dispositivos envíen y reciban información[15]. Esto incluye cualquier dispositivo inteligente en el hogar, electrodomésticos, bocinas, juguetes, objetos que se portan. Una pregunta común es "¿Alexa graba todas mis conversaciones?" El sitio web de Amazon indica que la respuesta es no. Explica que los dispositivos están diseñados para detectar únicamente la palabra que "despierta" al dispositivo (Alexa) y que identifican por medio de patrones acústicos que corresponden con esa palabra, así que ningún otro audio se almacena ni se envía a la "nube"[16]. Tenga en cuenta que al usar cualquier dispositivo que se conecta al internet hay un riesgo inherente de que una persona con malas intenciones pueda tener acceso a cierta información. Sin embargo, como siempre, recuerde no compartir ni almacenar información delicada o privada en internet.

<u>Botón para silenciar el micrófono y desconectar el dispositivo</u> Los dispositivos que responden a la voz tienen un botón silenciador integrado y cuando se activa, el dispositivo no responde aún si usted dice la palabra que lo despierta. Si usted quiere asegurarse por completo de que un dispositivo no está escuchando o grabando, puede desconectarlo o sacarle las baterías.

Protección del enrutador de WiFi. Los enrutadores inalámbricos ofrecen mucha libertad para las computadoras portátiles y los dispositivos móviles. Pero cuando usted compra un nuevo enrutador WiFi, con frecuencia ya contiene una configuración preestablecida que alguien puede averiguar o incluso adivinar. Asegúrese de cambiar la contraseña y cambiar el nombre de su red inalámbrica para que la fuente de internet que utiliza para sus dispositivos inteligentes sea segura [11].



Redes sociales y noticias falsas

Las redes sociales se han vuelto muy populares en los últimos años. Mientras que permiten que esté en contacto con sus amigos y familiares en cualquier momento y en cualquier lugar, sería mucho más seguro si tiene usted cuidado de lo que comparte con los demás en estas plataformas.

¡Esto es lo que puede hacer!

- ✓ **No acepte solicitudes de amistad de personas que no conoce**. Podría recibir mensajes de usuarios desconocidos que le ofrezcan regalos o boletos gratuitos como un anzuelo para que usted haga clic en sus enlaces o los conozca en persona. También sea cauteloso de los mensajes que anuncian productos o servicios en la sección de noticias. Nunca haga clic en enlaces sospechosos aún si parece que provienen de un amigo o una compañía conocida.
- ✓ **Sea consciente de cuánta información comparte**. Su perfil de las redes sociales en línea puede compartir gran cantidad de información. Esto puede incluir dónde vive, su fecha de nacimiento, sus preferencias, su familia y mucho más. Tenga cuidado con lo que publica. Esta información está destinada a sus amigos, pero los estafadores también la pueden ver dependiendo de su configuración de privacidad.
- ✓ **Pruebe otras alternativas al Facebook Messenger o el email**. Las aplicaciones cifradas como Signal, Whatsapp y ProntonMail proporcionan seguridad adicional.

✓ **Revise su configuración de privacidad**. En las plataformas de redes sociales como Facebook, usted puede configurar quién ve su información de perfil, lo que publica, su actividad, quién puede publicar en su página y quién puede etiquetarlo en fotos. Es buena idea establecer restricciones elevadas de privacidad para que pueda revisar en qué fotos y publicaciones ha sido etiquetado antes de que otras personas puedan verlas en su perfil.

Analicemos más de cerca

¿Le gusta hacer clic en "Me gusta"? Un botón que se ve como el botón de "Me gusta" en Facebook, o una imagen capturada de un vídeo que de inmediato captan su atención, podrían llevarlo involuntariamente a sitios de compras no deseados o incluso ocasionar la aparición de virus y malware.

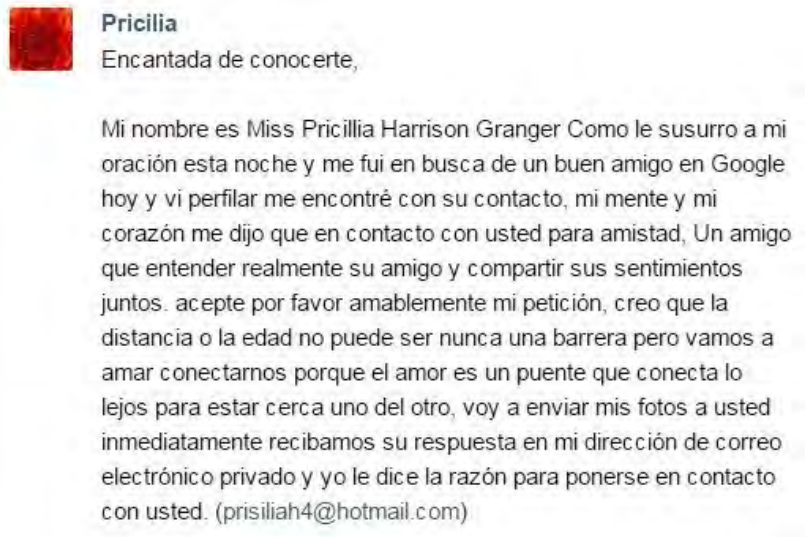
Es importante poder distinguir entre la apariencia de un botón de "Me gusta" auténtico que se ubica debajo de una publicación de Facebook y un botón engañoso que inicialmente se ve muy parecido. Los "ciberanzuelos" provocan curiosidad en los usuarios y los incita a hacer clic en un enlace, foto, vídeo o artículo en particular. Mientras que alguna de estas historias o anuncios engañosos simplemente nos llevan a otro sitio web, otros pueden ser dañinos. Sin embargo, al caer víctima del truco de dar al botón de "Me gusta" de un objeto, usted sin saberlo está propagando el mismo vídeo o imagen

Mire este enlace de referencia a la National Cyber Security Alliance—Stay Safe Online (Alianza Nacional de Ciberseguridad – Iniciativa de Seguridad en Línea) para manejar su configuración de privacidad en diferentes plataformas. **https://bit.ly/2BYiFVh**

Sitios de citas en línea. Las citas en línea pueden ser una gran herramienta para conocer nuevas personas con intereses similares, siempre que tenga cuidado sobre lo que decide compartir con los demás. Sea consciente de que hay muchos perfiles falsos en las aplicaciones de citas en los que tratarán de conseguir que haga clic a un enlace que lo dirija a algún sitio comprometedor.

¡Esto es lo que puede hacer!

- ✓ **Ponga atención a las señales de alerta en su perfil**. Al ponerse en contacto con alguien en las redes sociales o en las aplicaciones de citas, tenga presente que un nombre acompañado de una larga serie de números puede ser una señal de que se trata de un perfil falso. ¿El encabezado y el texto implican que solo están buscando algo físico?



Pricilia
Encantada de conocerte,

Mi nombre es Miss Pricillia Harrison Granger Como le susurro a mi oración esta noche y me fui en busca de un buen amigo en Google hoy y vi perfilar me encontré con su contacto, mi mente y mi corazón me dijo que en contacto con usted para amistad, Un amigo que entender realmente su amigo y compartir sus sentimientos juntos. acepte por favor amablemente mi petición, creo que la distancia o la edad no puede ser nunca una barrera pero vamos a amar conectarnos porque el amor es un puente que conecta lo lejos para estar cerca uno del otro, voy a enviar mis fotos a usted inmediatamente recibamos su respuesta en mi dirección de correo electrónico privado y yo le dice la razón para ponerse en contacto con usted. (prisiliah4@hotmail.com)

- ✓ **No haga clic en los enlaces que le envíen**. Después de varios intercambios de mensajes y cuando sienta que conoce a alguien, tal vez se sienta confiado de compartir su teléfono para acordar reunirse. Pero si no tiene una conversación sustanciosa y solo le envían un enlace, esto podría llevarlo a un sitio web lleno de malware y virus – evite hacer clic en enlaces como este y no tenga más contacto.

Noticias falsas. En las noticias y los medios hoy en día puede ser difícil descifrar qué es real y qué es falso. Ahora más que nunca las personas tienen más acceso a la información; sin embargo la verdad no siempre es clara puesto que cualquiera puede publicar lo que sea en internet y decir que es verdadero. ¿Cómo determinar si una fuente noticiosa es confiable?

¡Esto es lo que puede hacer!

- ✓ **Considere la fuente.** Cuando esté en un sitio web, reúna la información sobre el sitio en sí. Mire la sección “Acerca de nosotros”, ¿quién está a cargo del sitio? ¿Por qué han creado este sitio? ¿Quién paga por el sitio y favorecen a algún patrocinador? ¿De dónde proviene la información? Hay diferentes niveles de credibilidad que puede usted encontrar con solo fijarse en la parte final de la URL de un sitio web. Si la terminación es **.gov**, con frecuencia esto significa que se trata de un sitio gubernamental y en general deben pasar por varias revisiones y control de calidad antes de su publicación.

Si un sitio termina en.edu, significa que el sitio proviene de una escuela o universidad que generalmente se adhiere a estándares académicos para el material que publican.

✓ **Referencia cruzada**. Si consulta diferentes fuentes reconocidas y de buena reputación, sin tomar en cuenta el posible sesgo, ¿hay elementos comunes en la información? ¿Suena absurdo o como que es una broma? ¿Hay otras fuentes que verifiquen que la información es verdadera?

✓ **Investigue**. Revise la fecha para ver si la información es relevante a los eventos actuales. Pregunte a un experto cuando sea posible o consulte un sitio de verificación de los hechos.

Procedimiento de respuesta ante el fraude cibernético

Agencias responsables

Tipo de fraude	Agencia y contacto
Denuncias sobre estafas en general (Recomendado)	**Agencias policiales locales** La policía tiene la obligación de ayudarle y referirlo a otras agencias apropiadas.
Denuncias sobre estafas en general (Recomendado)	**Federal Trade Commission (Comisión Federal de Comercio)** Teléfono: 1-877-382-4357 (TTY/TTD: 1-866-653-4261)
Crimen y fraude en internet (Recomendado)	**Internet Crime Complaint Center** (IC3, Centro de Quejas de Crimen por Internet) surge de una colaboración entre el Federal Bureau of Investigation (FBI, Oficina Federal de Investigaciones) y el National White Collar Crime Center (NW3C, Centro Nacional de Delitos de Cuello Blanco). Denuncie cualquier crimen o fraude que ocurra en internet. http://www.ic3.gov/default.aspx
Denuncia de estafas relacionadas con la salud	**Llame a la Federal Trade Commission (FTC)** al 1-877-FTC-HELP (1-877-382-4357) o TTY 1-866-653-4261 O visite: ftc.gov/complaint
Fraude de Medicare	**Department of Health and Human Services (Departamento de Salud y Servicios Humanos)** Teléfono: 1-800-633-4227 Denuncie fraude, pérdidas y abuso de Medicare y Medicaid. Teléfono: 1-877-808-2468 **Senior Medicare Patrol (Patrulla de Adultos Mayores de Medicare)** www.smpresource.org **Office of the Inspector General (Oficina del Inspector General)** 1-800-447-8477 o envíe un email a spoof@oig.hhs.gov
Crimen de robo de identidad	**Identity Theft Resource Center (Centro de Recursos para el Robo de Identidad)** Teléfono: 1- 888-400-5530 http://www.idtheftcenter.org/knowledge-base/
Problemas relacionados con la salud para hispanoparlantes	**Su Familia: The National Hispanic Family Health Helpline (Línea de Ayuda Nacional para Familias Hispanas sobre la Salud)** Lunes a viernes de 9 am a 6 pm (EST) Teléfono: 1-866-Su-Familia (1-866-783-2645)
Fraude fiscal y del IRS (Oficina de Impuestos)	**IRS's Identity Protection Specialized Unit (Unidad Especializada en Protección contra el robo de Identidad)** Teléfono: 1-800-908-4490 **Oficina de Impuestos** Si usted o alguien que usted conoce ha recibido un email de alguien que dice ser de la Oficina de Impuestos y le pide información personal o financiera, reenvíe ese email al Internal Revenue Service (Oficina de Impuestos) a phishing@irs.gov.

Tipo de fraude	Agencia y contacto
Fraude fiscal y del IRS (Oficina de Impuestos)	**IRS's Identity Protection Specialized Unit (Unidad Especializada en Protección contra el robo de Identidad)** Teléfono: 1-800-908-4490 **Oficina de Impuestos** Si usted o alguien que usted conoce ha recibido un email de alguien que dice ser de la Oficina de Impuestos y le pide información personal o financiera, reenvíe ese email al Internal Revenue Service (Oficina de Impuestos) a phishing@irs.gov.
Estafa de lotería	**AARP Fraud Fight Call Center (Centro de Llamadas Contra el Fraude de AARP)** Denuncie cualquier estafa de lotería extranjera. Teléfono: 1-800 646-2283 **U.S. Postal Inspection Service (Servicio de Inspección Postal de Estados Unidos)** Denuncie cualquier estafa postal o de lotería 1-877-876-2455
Fraude de Seguro Social	**Social Security Administration (Administración del Seguro Social)** Teléfono: 1-800-269-0271 (TTY: 1-866-501-2101) 10:00 am a 4:00 pm (EST) http://oig.ssa.gov/report/
Fraude de pasaporte	**Department of the State (Departamento de Estado)** Contacte a PassportVisaFraud@state.gov
Fraude de negocios	**Better Business Bureau (Oficina para Mejores Negocios)** Presente una denuncia en su sitio web. https://www.bbb.org/consumer-complaints/file-a-complaint/get-started
Denuncie emails de phishing	**Department of Homeland Security, U.S. Computer Emergency Readiness Team (Departamento de Seguridad Nacional, Equipo de Preparación para Emergencias Informáticas de los Estados Unidos)** Email: phishing-report@us-cert.gov O presente una denuncia ante la Federal Trade Commission en spam@uce.gov También puede reenviar los emails de phishing a spam@uce.gov
Denuncias de abuso general contra adultos	**Adult Protective Services (Servicios de Protección para Adultos)** bajo el California Department of Social Services (Departamento de Servicios Sociales de California) brinda apoyo para las personas mayores y adultos dependientes. Denuncie si sospecha de abuso físico, sexual, auto negligencia, abandono, abuso financiero, psicológico y negligencia por parte de terceros. Para mayor información, visite http://www.cdss.ca.gov/Adult-Protective-Services El número telefónico varía en cada condado de California: http://www.cdss.ca.gov/inforesources/County-APS-Offices

Recursos

Si le interesa conocer más sobre la seguridad en línea o si desea enseñar a otros sobre este tema, esta lista de recursos puede ser útil.

Nombre	Sitio web
AARP (American Association of Retired Persons) (Asociación Estadounidense de Personas Jubiladas) le ofrece las noticias más recientes sobre las estafas dirigidas a los adultos mayores.	http://www.aarp.org/money/scams-fraud/ Hay voluntarios capacitados en consejería sobre fraude disponibles en su línea directa al teléfono 1 (877) 908-3360.
CFTC (Commodity Futures Trading Commission) (Comisión del Comercio en Futuros sobre Mercancía) informa al consumidor sobre fraudes en el mercado de contratos futuros de Estados Unidos.	http://www.cftc.gov/ConsumerProtection/Resources/index.htm
Consumer Financial Protection Bureau (Oficina de Protección Financiera al Consumidor) ofrece información sobre estafas financieras y productos financieros engañosos.	http://www.consumerfinance.gov/
FBI (Federal Bureau of Investigations) (Oficina Federal de Investigaciones) brinda información sobre los fraudes que se valen de los medios masivos para engañar al consumidor.	https://bit.ly/2rWBZOK
ElderCare.gov lo conecta con servicios comunitarios para adultos mayores, incluyendo servicios de ayuda financiera y legal.	https://eldercare.acl.gov/Public/Index.aspx
Federal Trade Commission (Comisión Federal de Comercio) le brinda información sobre fraudes nuevos y actuales y también ofrece consejos para ayudarlo a estar protegido.	http://www.consumer.ftc.gov/scam-alerts Vea esta campaña de concienciación de estafas en línea de la FTC: http://www.consumer.ftc.gov/features/feature-0030-pass-it-on
Federal Housing Finance Agency (Agencia Federal de Finanzas de Vivienda) brinda consejos para ayudar a los consumidores a evitar estafas relacionadas con la vivienda, tales como estafas de rescate de hipoteca, estafas de bancarrota y fraude de hipotecas inversas.	https://www.fhfa.gov/
U.S. Bureau of Consular Affairs (Oficina de Asuntos Consulares) brinda información a los estadounidenses que son víctimas de un crimen en el extranjero.	http://travel.state.gov/content/passports/english/go.html

Nombre	Sitio web
Internet Crime Complaint Center (Centro de Quejas de Crímenes por Internet) surge de una colaboración entre el FBI y el National White Collar Crime Center y remite las denuncias a las agencias reguladoras federales, estatales, locales o fuerzas del orden internacional.	http://www.ic3.gov/crimeschemes.aspx
Oasis promueve el aprendizaje continuo para los adultos mayores y ofrece recursos sobre la ciberseguridad.	https://bit.ly/2RrFnQh
Elder Justice Initiative (Iniciativa de Justicia para Ancianos) proporciona información del Departamento de Justicia de Estados Unidos relacionada con los adultos mayores, víctimas de abuso y explotación financiera y sus familias.	http://www.justice.gov/elderjustice/
Stay Safe Online by National Cyber Security Alliance (Esté Seguro en Línea de la Alianza Nacional de Ciberseguridad) proporciona consejos y recursos para que usted y su familia estén protegidos.	https://www.staysafeonline.org/stay-safe-online/resources/
GCF Global ofrece recursos de seguridad en internet.	https://edu.gcfglobal.org/en/internetsafety/
Medicare.gov proporciona información sobre lo que puede hacer para mantener su información personal segura y prevenir el fraude de Medicare.	https://www.medicare.gov/forms-help-resources/help-fight-medicare-fraud

Fuentes

[1] Anderson, Monica and Andrew Perrin. "Technology Use Among Seniors." *Pew Internet Center*, 17 May. 2017. Web. 31 Dec. 2018. http://www.pewinternet.org/2017/05/17/technology-use-among-seniors/

[2] New York State Office of Children and Family Services "Under the Radar: The New York State Elder Abuse Prevalence Study." *Self Reported Prevalence and Documented Case Surveys Final Report*2011. Web. 31 Dec. 2018. https://ocfs.ny.gov/main/reports/Under%20the%20Radar%2005%2012%2011%20final%20report.pdf

[3] Office of Financial Protection for Older Adults "Suspicious Activity Reports on Elder Financial Exploitation: Issues and Trends." *Consumer Financial Protection Bureau*, February 2019. Web. 12 March 2019. https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_suspicious-activity-reports-elder-financial-exploitation_report.pdf

[4]Baig, Mehroz. “Elder Abuse and Technology.” *The Commonwealth Blog*, 6 Jun. 2013. Web. 4 Jan. 2016. http://www.commonwealthclub.org/blog/2013-06-06/elder-abuse-and-technology

[5]VanDeVelde, Amy. “Oasis YouTube video provides great guidance on how to navigate and trust what you hear on the news.” *Oasis Blog*, 14 March 2018. Web. 31 Dec. 2018. https://www.oasisnet.org/Blog/is-it-fake-news-find-out-how-to-know-for-sure-151661?utm_source=Center+0&utm_medium=email&utm_campaign=7585+March+2018+Discoveries&utm_term=620598

[6] Federal Trade Commission. "Health Care Scams." *Pass It On Resource Guide*, 2014. Web. 31 Dec. 2018. https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0183-health-care-scams.pdf

[7]Sjouwerman, Stu. “Scam Of The Week: New FBI and IRS Alerts Against W-2 Phishing.” *KnowB4 Security Awareness Training Blog*, 18 March. Web. 31 Dec. 2018. https://blog.knowbe4.com/scam-of-the-week-new-fbi-and-irs-alerts-against-w-2-phishing

[8]The Office of Investor Education and Advocacy (OIEA). “Investor Alert: Prime Bank Investments Are Scams.” U.S. Securities and Exchange Commission, 5 Feb. 2015. Web. 4 Jan. 2016. http://www.sec.gov/oiea/investor-alerts-bulletins/ia_primebankscam.html

[9]The Federal Bureau of Investigation. “Common Fraud Schemes.” *Scams& Safety*, 2010. Web. 4 Jan. 2016. https://www.fbi.gov/scams-safety/fraud

[10] AARP. “Prevention, Not Just Awareness, Key to Cyber Security.” Web. 31 Dec. 2018. https://states.aarp.org/prevention-awareness-cyber-security/

[11]StaySafe Online. “Shopping Online.” *Online Safety Basics*. Web. 31 Dec. 2018. https://staysafeonline.org/stay-safe-online/online-safety-basics/online-shopping/

[12]Kirchheimer, Sid. "Is Your Computer Infected." *AARP*, 9 Jan. 2012. Web. 31 Dec. 2018. https://www.aarp.org/money/scams-fraud/info-01-2012/computer-infected-scam-alert.html

[13]VanDeVelde, Amy. “Two factor authentication adds an essential layer of security.” *Oasis Blog*, 17 October 2017. Web. 31 Dec. 2018. https://www.oasisnet.org/Blog/want-more-protection-for-your-email-and-facebook-accounts-135523

[14]National Cyber Security Alliance. “Cheers to Safe Cybershopping!” *Stay Safe Online*. Web flyer. 31 Dec. 2018. https://staysafeonline.org/wp-content/uploads/2018/11/Online-shopping-tip-sheet-1118.pdf

[15]“IOT.” *Merriam-Webster Dictionary*. https://www.merriam-webster.com/dictionary/Internet%20of%20Things

[16] Amazon.com. “Alexa and Alexa Device FAQS” Web. Feb. 2019. https://www.merriam-webster.com/dictionary/Internet%20of%20Things

Nuestra misión: Explorar el uso innovador de la tecnología para ayudar a las personas a prosperar al mejorar su bienestar e independencia, sobre todo conforme envejecemos.

Nuestra visión: La innovación tecnológica juega un papel importante para mejorar de la capacidad de cada persona de "vivir la vida a mi manera" en donde quiera que esté su hogar. Nuestra meta es aprovechar las soluciones de tecnología que apoyen y fomenten el bienestar y nos ayuden a prosperar en mente, cuerpo y espíritu.

Nuestros proyectos: Iniciativas que representan un rango diverso de tecnología e innovaciones que se concentran en áreas específicas como el fortalecimiento social y la conexión, la promoción de la participación significativa, el crecimiento y el completo bienestar de la persona, el avance del control proactivo y participativo sobre la salud y el bienestar, la expansión del apoyo para las capacidades de movilidad, visión, audición y cognición, la prevención de emergencias o eventos graves antes de que ocurran, la facilitación y el apoyo de los círculos de cuidado y promoción de ambientes sanos, seguros, accesibles y sustentables.

Para mayor información, por favor visite www.fpciw.org.

front porch

CENTER FOR INNOVATION AND WELLBEING