LA OPORTUNIDAD DE LA CONFIANZA:

EXPLORAR LAS ACTITUDES DE LOS CONSUMIDORES HACIA EL INTERNET DE LAS COSAS

CONSUMERS INTERNATIONAL

Internet Society

RESUMEN EJECUTIVO

Esta nueva investigación de Consumers International y la Internet Society exploró las percepciones y actitudes de los consumidores hacia la confianza, la seguridad y la privacidad de los dispositivos de Internet de las cosas (IoT) de los consumidores.

La encuesta de consumidores que se llevó a cabo en Australia, Canadá, Francia, Japón, el Reino Unido y los EE. UU. tuvo como objetivo averiguar qué es lo más importante para los consumidores al comprar dispositivos conectados y quién es el responsable de una mejor privacidad y seguridad.

Índice

Lo que descubrimos:

- Los dispositivos conectados están en todas partes, pero las preocupaciones acerca de la privacidad y la seguridad persisten.
- El 63 % de las personas encuestadas consideran que los dispositivos conectados son "perturbadores" por la forma en que recopilan datos sobre las personas y sus comportamientos.
- Este sentimiento se refleja en toda la encuesta, ya que la mitad de las personas en todos los mercados no confían en que sus dispositivos conectados protejan su privacidad y manejen su información de manera respetuosa (53 %).
- Además de no confiar en el dispositivo en sí mismo para mantener la seguridad de los datos, el 75 % de las personas coincide en que existe un motivo para preocuparse porque otras organizaciones utilizan sus datos sin su permiso.
- Los problemas de seguridad son lo suficientemente graves como para disuadir a casi un tercio (28 %) de las personas que no poseen dispositivos inteligentes a comprar uno; los problemas de seguridad son un disuasivo tan fuerte como el precio de un dispositivo.[1]
- Las personas están preocupadas por la seguridad y la privacidad, pero no saben cómo adaptar y ajustar la configuración del dispositivo de una manera que pueda disipar estos temores. El 80 % de las personas encuestadas saben cómo configurar y restablecer las contraseñas, pero solo el 50 % sabe cómo deshabilitar la recopilación de datos sobre los usuarios y sus comportamientos.

  Vemos en la encuesta que un número elevado considera que los reguladores (88 %) deben garantizar los estándares de privacidad y seguridad, seguidos por los fabricantes (81 %) y los comerciantes (80 %).

[1] Tenga en cuenta que las preocupaciones por la seguridad fueron disuasivos tan fuertes como el precio de un dispositivo en todos los mercados con excepción de Japón.

28%

DE LAS PERSONAS QUE NO POSEEN UN DISPOSITIVO INTELIGENTE, NO COMPRARÁN UNO DEBIDO A PROBLEMAS DE SEGURIDAD

63%

DE LAS PERSONAS ENCUENTRAN LOS DISPOSITIVOS CONECTADOS "PERTURBADORES"

50%

DE LAS PERSONAS SABEN CÓMO DESACTIVAR LA RECOPILACIÓN DE DATOS

75%

DE LA DESCONFIANZA DE LAS PERSONAS ES LA FORMA CÓMO SE COMPARTEN LOS DATOS

Dado el nivel de preocupación entre propietarios y no propietarios, existe la posibilidad de que las empresas utilicen altos niveles de privacidad y seguridad como una forma de diferenciarse y generar confianza con los clientes actuales y futuros, al mismo tiempo que crean un entorno de IoT más seguro para el consumidor.

Los resultados[2] también sugieren que los consumidores piensan en la necesidad de una reglamentación más formal en el mercado. Es probable que esta demanda crezca a medida que la información sobre los riesgos asociados con los productos conectados se generalice.

En respuesta a esta demanda, las empresas deben explorar cómo ofrecer garantías a los consumidores de que sus dispositivos y servicios son útiles y ayudan sin cruzar la línea hacia lo perturbador.

Esto podría ayudarlos a generar confianza entre los consumidores hacia los dispositivos conectados y posiblemente generar una ventaja competitiva.

[2] Como los resultados se basan en preguntas directas sobre el riesgo y la preocupación por los productos de IoT, se debe tener en cuenta que no podemos determinar en qué medida estas preocupaciones son siempre importantes, pero cuando se mencionaron hubo una preocupación generalizada sobre la seguridad y la privacidad.

SOBRE LA ASOCIACIÓN Y EL PROYECTO

CONSUMERS INTERNATIONAL

Consumers International es la organización global de membresía para grupos de consumidores en todo el mundo. Unimos a más de 200 organizaciones miembro en más de 100 países para empoderar y defender los derechos de los consumidores en todas partes. Queremos que los consumidores obtengan el mayor provecho de la economía y la sociedad digital sin tener que sacrificar la calidad, el cuidado y el trato Justo.

Internet Society

Fundada por pioneros de Internet, la Internet Society es una organización sin fines de lucro dedicada a asegurar el desarrollo, evolución y uso de Internet. Al trabajar a través de una comunidad global de capítulos y miembros, la Internet Society colabora con una amplia variedad de grupos para promover las tecnologías que aportan seguridad a Internet y abogan por las políticas que facilitan el acceso universal.

Consumers International y la Internet Society están trabajando en sociedad para ofrecer un mejor mundo digital, donde todos se puedan beneficiar de la innovación digital sin comprometer sus derechos. Ambos consideramos que la seguridad y la privacidad en línea son claves para la confianza en línea, lo que sustenta todos los intercambios económicos y sociales en línea.

La asociación reúne el mejor conocimiento técnico y de políticas relacionado con IoT de Internet Society y el conocimiento de larga data de las experiencias y actitudes de los consumidores hacia la economía digital y la sociedad de Consumers International.

El foco de nuestra asociación ha estado en el creciente mercado del IoT para el consumidor como una parte importante del entorno digital de las personas. Hemos estado trabajando para lograr la participación efectiva de los consumidores, los gobiernos y los reguladores, y las empresas en la creación de un mercado de IoT seguro y confiable. Queremos permitir que los grupos de consumidores de todo el mundo ayuden a impulsar la demanda de mayor seguridad y privacidad en los productos de IoT para los consumidores.

Esta investigación es una parte clave de esta actividad, ya que explora lo que los consumidores actualmente entienden y sienten acerca de la confianza, la seguridad y la privacidad en el IoT del consumidor y cómo un cambio en las políticas, nuevas prácticas comerciales, desarrollo de estándares y cumplimiento, junto con la sensibilización entre los consumidores, pueden aportar un cambio positivo.

Oportunidades de seguridad y privacidad en el mercado de IoT de los consumidores

El rápido aumento de los productos y servicios que están conectados a Internet ya está transformando las vidas de los consumidores a través de redes eléctricas conectadas, transporte, seguridad del hogar y accesorios adaptados al estilo de vida. Los pronósticos predicen que esta tecnología se convertirá en parte de la vida cotidiana con muchos productos conectados a Internet de manera predeterminada.

Las pruebas realizadas por organizaciones de consumidores han revelado peligrosas deficiencias en la gama de productos conectados, desde juguetes para niños y relojes conectados hasta televisores conectados y medidores de actividad. Dichas vulnerabilidades crean el riesgo de exponer el dispositivo en sí (por ejemplo, un bloqueo del hogar conectado que se deshabilita) y de los datos personales (por ejemplo, la información que se comparte con terceros no autorizados). Al pensar más allá del daño a los consumidores, las vulnerabilidades de IoT también crean el riesgo de exponer redes (por ejemplo, atacar la red eléctrica de todo un país a través de cámaras web conectadas).

> “UNA PRUEBA REALIZADA POR ORGANIZACIONES DE CONSUMIDORES HA REVELADO DEBILIDADES PELIGROSAS EN UN RANGO DE PRODUCTOS CONECTADOS.”

> “LA FALTA DE CONFIANZA DE LOS CONSUMIDORES EN EL MERCADO DE IOT PODRÍA SER PERJUDICIAL PARA LOS FABRICANTES Y COMERCIANTES.”

A medida que más tipos de dispositivos y servicios conectados por defecto se generalizan para los consumidores, estos problemas de seguridad y privacidad se multiplican. Estos problemas representan una amenaza no solo para el control de los consumidores sobre lo que sucede con sus datos, sino también para la confianza de los consumidores en los dispositivos de IoT. La falta de confianza de los consumidores en el mercado de IoT podría ser perjudicial para los fabricantes y comerciantes y, como resultado, podría frenar la innovación dentro de la industria. Creemos que hay oportunidades para que diferentes partes interesadas aborden los problemas de seguridad y privacidad en el mercado de IoT y aumenten la confianza del consumidor.

Comprender actitudes y recoger opiniones

Al complementar nuestras otras actividades con fabricantes, comerciantes y reguladores dentro de esta asociación, esta encuesta brinda una valiosa perspectiva del consumidor que nos permitió obtener información no solo sobre cómo los consumidores perciben los dispositivos IoT, sino también sus niveles de conocimiento e ideas sobre la responsabilidad.

Este estudio tuvo como objetivo conocer las actitudes de los consumidores hacia la privacidad y la seguridad cuando se trata de dispositivos conectados y explorar en qué medida los consumidores confían en los dispositivos conectados. Nuestros otros objetivos fueron comprender qué es importante para los consumidores cuando compran dispositivos conectados y dónde creen que debería recaer la responsabilidad de una mejor seguridad y privacidad.

[3] Vea por ejemplo la actividad de nuestros miembros noruegos y belgas:
https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/
https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/
https://www.test-aankoop.be/action/pers%20informatie/persberichten/2018/hackable-home
https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/

Metodología

La investigación fue llevada a cabo por Ipsos MORI a través de su encuesta de panel en línea que regularmente examina a la población general en línea en todo el mundo.

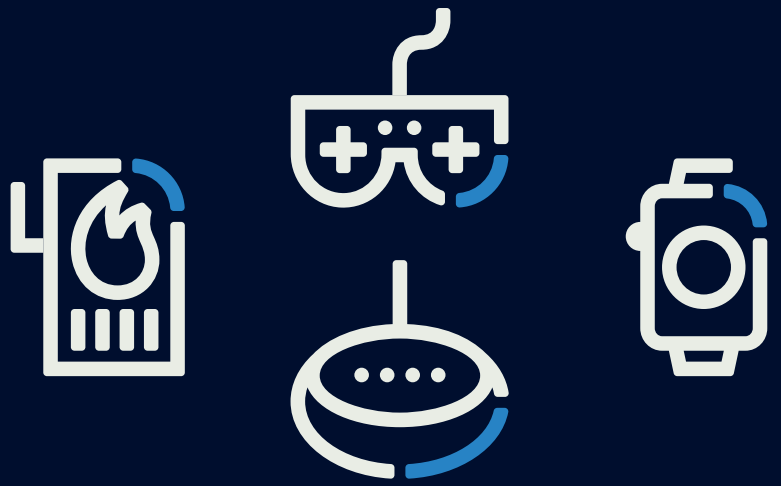
Encuestamos una muestra de un mínimo de 1,000 consumidores en cada uno de estos países: Estados Unidos, Francia, Canadá, Australia, Reino Unido y Japón entre el 1 de marzo y el 6 de marzo de 2019. Elegimos realizar la encuesta en línea para asegurarnos de que las muestras de cada país reflejaran la población general en línea. Las personas que están en línea tienen más probabilidades de entender cómo funcionan estos dispositivos. El estudio no requería que las personas tuvieran un dispositivo conectado, por lo que también reflejó la opinión de los consumidores que están considerando comprar o no han comprado un dispositivo.

Desentrañar las complejidades de la confianza del consumidor en los dispositivos conectados y lo que la sustenta puede ser una tarea difícil, especialmente en el contexto de una encuesta cuantitativa que puede restringirse en términos de la profundidad de los conocimientos. Los conceptos de confianza y dispositivos conectados pueden ser abstractos y varían en la interpretación de cada uno por parte de las personas.
El estudio trató de mitigar esta difícil posición al captar las actitudes de los consumidores hacia la confianza en los dispositivos conectados al incitarlos con declaraciones de actitud sobre dichos dispositivos. Las declaraciones fueron precedidas por una definición y ejemplos de dispositivos conectados.

Definir a los dispositivos inteligentes

Para esta investigación, definimos a los dispositivos inteligentes como productos cotidianos que pueden conectarse a Internet mediante WiFi o Bluetooth, como medidores conectados, monitores de actividad física, juguetes conectados, asistentes domésticos o consolas de juego.[4]

La definición excluye tabletas, teléfonos móviles y computadoras portátiles; si bien pueden considerarse "dispositivos conectados" en términos de tecnología, son mucho más complejos y las aplicaciones les permiten realizar muchas funciones que a su vez generan problemas de privacidad y seguridad más complejos que otros dispositivos conectados. Para evitar confundir los asuntos, la investigación se centró en los dispositivos que no tienen esta capa adicional de complejidad.



[4] Al indicar a los encuestados sobre lo que entendemos por dispositivos conectados, aseguramos la coherencia y la alineación en la comprensión, y por lo tanto la capacidad de inferir y generalizar en todos los mercados. Se realizaron traducciones del cuestionario original al francés (en sus versiones canadiense y francés) y japonés. Se empleó una revisión local para garantizar la coherencia en las diferencias locales, en términos como "perturbador", "preocupación", "riesgo" y ejemplos de dispositivos conectados.

HALLAZGOS DE LA INVESTIGACIÓN

1 INMERSOS EN LAS CUESTIONES DE PRIVACIDAD Y SEGURIDAD

Los dispositivos de IoT para el consumidor son ampliamente utilizados: la encuesta mostró que el 69 % de los participantes en todos los mercados poseen uno o más dispositivos como medidores conectados, monitores de actividad física, juguetes conectados, asistentes domésticos o consolas de juegos.

Nuestros participantes en todos los mercados poseen con mayor frecuencia consolas de juego, seguidos de electrodomésticos y monitores de actividad física. En promedio, poseen dispositivos conectados de al menos dos categorías diferentes (por ejemplo, electrodomésticos y dispositivos portátiles conectados); sin embargo, este número es más bajo en Japón, donde el 46 % no posee ningún dispositivo conectado a Internet.

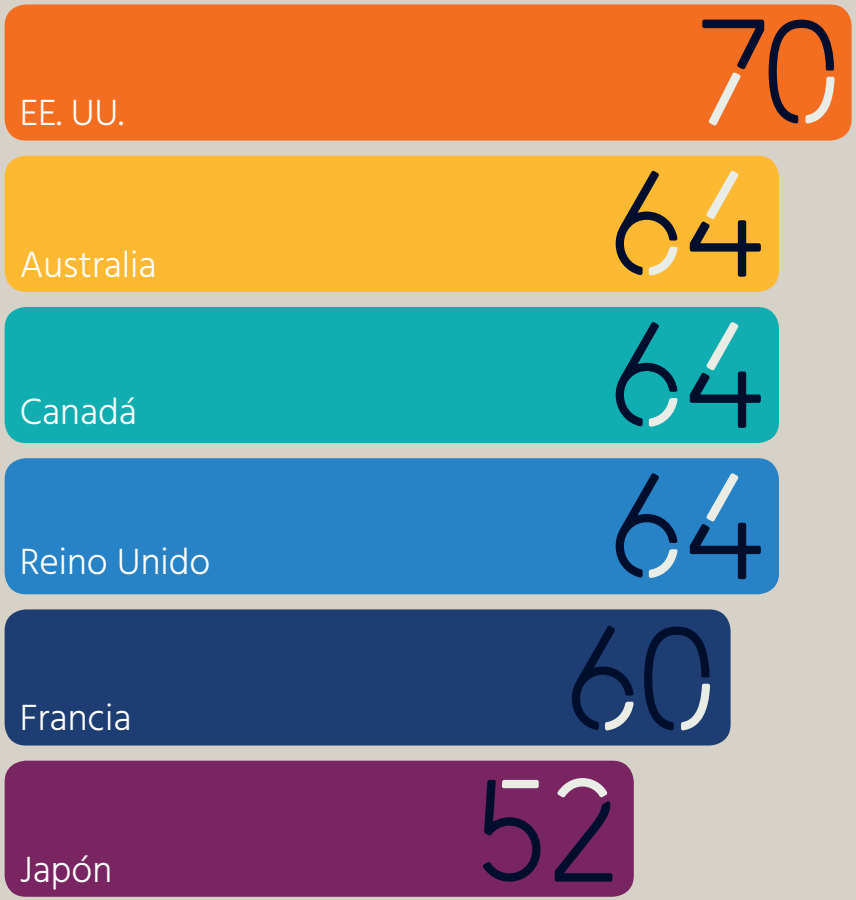
También hemos aprendido que los altos niveles de propiedad de dispositivos conectados no indican que las personas estén satisfechas con la privacidad y seguridad de estos dispositivos. En promedio, el 65 % de los consumidores en todos los mercados informan que están preocupados por la forma en que los dispositivos conectados recopilan y usan datos personales, y los Estados Unidos muestran los niveles más altos de preocupación con un 70 %.

Por otro lado, los consumidores en Francia (60 %) y Japón (52 %) muestran menos preocupación por la forma en que estos dispositivos recopilan y utilizan los datos, que el resto de los países encuestados. A modo de comparación, preguntamos sobre otras formas de tecnología y encontramos que las aplicaciones móviles (como las aplicaciones bancarias o de salud) tenían los niveles más altos de preocupación sobre la forma en que se recopilan los datos personales (69 %). El nivel más bajo de preocupación encontrado fue para las tabletas o las computadoras portátiles, que preocupa al 62 % de las personas.

65 %

DE TODOS LOS MERCADOS SE PREOCUPAN POR LA FORMA EN QUE LOS DISPOSITIVOS CONECTADOS RECOPILAN Y UTILIZAN DATOS PERSONALES.

PREOCUPACIÓN POR LA FORMA EN QUE LOS DISPOSITIVOS CONECTADOS RECOPILAN Y UTILIZAN LOS DATOS PERSONALES:



En todos los países estas preocupaciones son compartidas por aquellos que no han comprado un dispositivo. Queríamos descubrir si las intenciones de los consumidores de comprar o no comprar un dispositivo conectado están relacionadas con sus preocupaciones sobre privacidad y seguridad. Si bien las barreras que se mencionaron más frecuentemente para comprar un dispositivo conectado en todos los países son la falta de necesidad/uso para ellos (63 %) y el costo (28 %), la investigación también encontró que el 28 % de las personas que no son propietarias y no tienen la intención de comprar un dispositivo conectado toma esta decisión debido a la falta de confianza en la seguridad y la privacidad.

¿La oportunidad para la confianza?

No debería sorprender que si se fabricaran dispositivos útiles, asequibles, respetuosos de la privacidad y la seguridad resultarían populares entre los consumidores, pero aún no hemos visto que muchas compañías incorporen de forma voluntaria características sólidas de privacidad y seguridad en sus productos.

Dado el nivel de preocupación entre propietarios y no propietarios, las empresas podrían usar esto como una forma de diferenciarse de la multitud y generar confianza para los clientes actuales y futuros, y crear un entorno más seguro de IoT para el consumidor. Si tenemos en cuenta el enfoque que los fabricantes y comerciantes ponen en el precio de un producto conectado como una forma de influir en el comportamiento de compra de los consumidores, de nuestra investigación se desprende que los buenos estándares de privacidad y seguridad en un dispositivo de IoT pueden ser un punto de venta y un diferenciador competitivo igualmente importantes.

2 TEMOR Y DESCONFIANZA

Los conceptos y definiciones como la confianza, Internet de las cosas o incluso la privacidad y la seguridad pueden ser difíciles de explorar entre los consumidores debido a su naturaleza abstracta. En particular, al tratar de obtener más información sobre la confianza de los consumidores en la seguridad y la privacidad de los dispositivos de IoT, tuvimos que superar el obstáculo de tratar de explicar qué entendemos por "confianza".

Personas de diferentes orígenes y culturas pueden interpretar un concepto como la confianza de muchas maneras. Para mitigar las diferencias, les pedimos a los participantes que expresaran su opinión sobre una serie de afirmaciones que podrían relacionarse con sus sentimientos de confianza.

Nuestros resultados mostraron que el 63 % de las personas coinciden en que los dispositivos conectados son perturbadores[5] porque recopilan datos de las personas y sus comportamientos, siendo los consumidores franceses los más "perturbados" (71 %) y los japoneses los menos (46 %). Esta emoción se reflejó nuevamente cuando preguntamos acerca de la posibilidad de que otras organizaciones accedan a los datos de los dispositivos de IoT sobre los usuarios sin permiso, por ejemplo, los anunciantes que hacen un mal uso de los datos que los consumidores pensaban que se estaban recopilando para un propósito diferente. De hecho, tres cuartas partes de los consumidores en todos los países encuestados estaban preocupados por esta práctica cuando se trata de dispositivos conectados.

63 % **DE LAS PERSONAS COINCIDEN EN QUE LOS DISPOSITIVOS CONECTADOS SON PERTURBADORES EN LA FORMA CÓMO RECOPILAN DATOS**

> "DESARROLLAR LA CONFIANZA CON LOS CLIENTES ACTUALES Y FUTUROS ES UNA MANERA PARA QUE LAS EMPRESAS PUEDAN SOBRESALIR ENTRE LA MULTITUD."

Los consumidores no solo desconfían de la seguridad de los dispositivos de IoT para protegerlos de otras partes que acceden a sus datos, sino que incluso desconfían del dispositivo en sí. En los mercados, más de la mitad de las personas tienden a desconfiar de que sus dispositivos conectados protegen su privacidad y manejan su información de manera respetuosa (53 %). En Francia, la cantidad de personas que no confía en que sus dispositivos los protegen es el 63 %.

A pesar de que los consumidores son propietarios de dispositivos IoT y se comprometen con ellos, lo hacen con una nube de sospecha a su alrededor y experimentan desconfianza hacia el dispositivo en varios niveles.

¿La oportunidad para la confianza?

Existe una oportunidad real para que las empresas reconsideren cómo pueden fomentar la confianza de los consumidores en el mercado de IoT. Las empresas, ya sean fabricantes o comerciantes, deben explorar cómo brindar garantías a los consumidores de que sus dispositivos y servicios son útiles y ayudan sin cruzar la línea hacia lo perturbador que podría contribuir a generar sentimientos de desconfianza.

En términos prácticos, pueden establecer expectativas adecuadas respecto a qué datos se recopilan, cómo se utilizan y cómo se aseguran. Las empresas pueden resaltar características que pueden ser controladas por el consumidor, como habilitar o deshabilitar la recopilación de datos.

[5] Se realizaron traducciones del cuestionario original al francés (en sus versiones canadiense y francés) y japonés. Se empleó una revisión local para garantizar la coherencia en las diferencias locales, en términos como "perturbador", "preocupación", "riesgo" y ejemplos de dispositivos conectados.

3 POCO CONOCIMIENTO ESPECIALIZADO

Explorar los conceptos de privacidad y seguridad en dispositivos conectados entre consumidores no ha sido sencillo. Es difícil separar los dos y señalar dónde termina la privacidad y comienza la seguridad. Los dos tienden a trabajar juntos en un nivel conceptual más alto con el que la mayoría de los consumidores no se involucra a diario. Por este motivo, la investigación exploró el conocimiento del consumidor de los dos conceptos a través de las características de privacidad y seguridad de los dispositivos IoT.

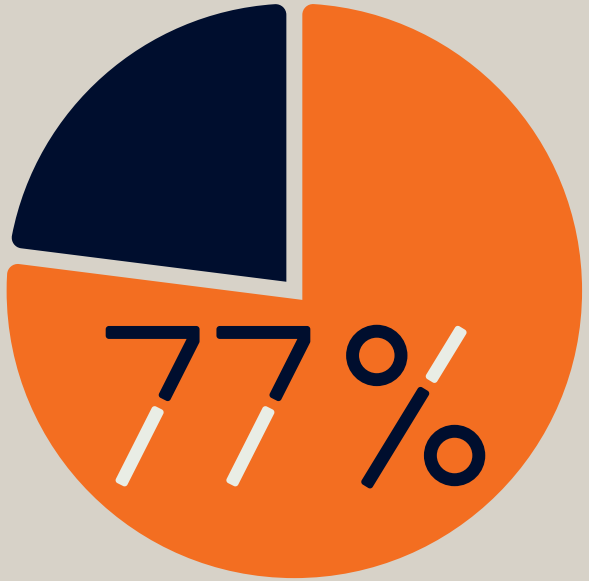
Descubrimos que las personas están preocupadas por la seguridad y la privacidad, pero no saben cómo adaptar y ajustar la configuración del dispositivo de una manera que pueda disipar estos temores. Existe un buen conocimiento de las mejores prácticas de seguridad básicas, como establecer y restablecer contraseñas. El 80 % de las personas encuestadas saben cómo configurar y restablecer las contraseñas y el 68 % de las personas conocen las actualizaciones de seguridad automáticas de los fabricantes. El conocimiento de estas características es esencial para mitigar los ataques y disminuir el impacto de los ataques cibernéticos. Sin embargo, se sabe mucho menos sobre otras configuraciones en los dispositivos. Solo el 50 % de los consumidores conoce las configuraciones que controlan qué datos se recopilan y con quién se comparten.

La investigación mostró que, en general, los consumidores en Australia, Reino Unido, Estados Unidos y Canadá conocen mucho mejor las características de seguridad en los dispositivos conectados que los consumidores en Japón y Francia. Sin embargo, la única característica de seguridad en la que los cuatro países están tan inseguros como Francia y Japón es en la deshabilitación de la recopilación de datos en sus dispositivos conectados.

> “SOLO EL 50 % DE LOS CONSUMIDORES CONOCEN LAS CONFIGURACIONES QUE CONTROLAN LA RECOPILACIÓN DE DATOS.”

A pesar de que los consumidores tienen poco conocimiento de ciertas características de seguridad en los dispositivos conectados, tienen un deseo de seguridad y privacidad como conceptos más amplios. Es posible que no estén al tanto de algunas características, pero han evaluado que la privacidad y la seguridad son un componente importante de los dispositivos de IoT y, como consumidores, deben conocerlos. Nuestra investigación demostró que la disponibilidad de información sobre la privacidad y seguridad del dispositivo conectado es parte de la ecuación de compra, con el 77 % de las personas en todos los mercados que considera que la disponibilidad de información sobre la privacidad y seguridad de un dispositivo conectado es importante para su decisión de compra.

Entre los países encuestados, la cantidad de consumidores de EE. UU. que tienen en cuenta la información de privacidad y seguridad de un dispositivo conectado al realizar una compra fue la más alta (82 %). En contraste, solo el 61 % de los consumidores franceses buscan esta información cuando compran un dispositivo de IoT, seguido por los consumidores japoneses con el 70 %.



LA DISPONIBILIDAD DE LA INFORMACIÓN SOBRE PRIVACIDAD Y SEGURIDAD ES UNA PARTE DE SU DECISIÓN DE COMPRA

PORCENTAJE DE CONSUMIDORES QUE ESTUVIERON DE ACUERDO CON CADA AFIRMACIÓN EN RELACIÓN CON LA COMPRA DE UN DISPOSITIVO CONECTADO

¿Qué influye en los consumidores para comprar o no comprar IoT?

Investigamos qué factores influyeron en los consumidores cuando decidieron comprar o no un dispositivo conectado. A los encuestados se les mostró una lista de ocho factores potenciales, y se les preguntó con cuáles estaban de acuerdo. El gráfico opuesto muestra el porcentaje de consumidores que estuvieron de acuerdo con cada afirmación. Estos resultados muestran que una combinación de los ocho factores se consideró importante, lo que indica un proceso complejo de toma de decisiones.

¿La oportunidad para la confianza?

Mejorar el conocimiento de las características de privacidad y seguridad entre los consumidores podría ayudar de alguna manera a que los consumidores se sientan menos preocupados por la forma en que su información personal se utiliza para cosas como marketing o mejoras de servicio.

4 ¿DÓNDE RECAE LA RESPONSABILIDAD?

Pedirle a los consumidores que asignen responsabilidades de seguridad y privacidad puede ser problemático. A menudo solo tienen conocimientos básicos sobre temas relacionados con IoT y una falta de una imagen más amplia del mercado de IoT. Sin embargo, lo que las personas pueden hacer es indicar si consideran que deberían tener la responsabilidad como consumidores.

Nuestra encuesta mostró que aproximadamente el 60 % de las personas en todos los mercados piensan que los consumidores deberían ser responsables de la seguridad y la privacidad en sus dispositivos conectados. Francia tuvo el número más bajo de personas que querían asumir la responsabilidad de la seguridad y la privacidad en los dispositivos de IoT (48 %). Sin embargo, incluso este número muestra que los consumidores como usuarios principales de dispositivos de IoT comparten la responsabilidad de la seguridad y la privacidad.

Sin embargo, la mayoría de las personas está de acuerdo en que los reguladores (88 %) deben garantizar niveles adecuados de privacidad y seguridad, seguidos por los fabricantes (81 %) y favorecidos por los comerciantes (80 %). Esta tendencia difirió ligeramente solo en Japón, donde los consumidores tenían una mayor preferencia por establecer obligaciones legales, como la regulación para garantizar los estándares de seguridad y privacidad en los dispositivos de IoT.

Estos resultados no son una sorpresa después de los hallazgos anteriores que muestran que los consumidores no tienen un conocimiento muy sofisticado sobre la seguridad y privacidad en los dispositivos de IoT. El nivel de riesgo de los dispositivos y la complejidad de la seguridad de los dispositivos contribuye a que los consumidores deseen que los reguladores, fabricantes y comerciantes respeten los estándares de privacidad y seguridad y asuman una mayor responsabilidad, como es el caso de otras actividades principales que presentan riesgos potencialmente altos para los individuos: como la seguridad de los viajes aéreos.

PORCENTAJE DE CONSUMIDORES QUE COINCIDEN CON CADA AFIRMACIÓN:

¿La oportunidad para la confianza?

Predecimos que la demanda de una regulación más formal por parte de los consumidores crecerá a medida que la información sobre los dispositivos conectados se generalice y que los medios detecten ataques de alto perfil y fallas de seguridad. Hasta que esto suceda, los comerciantes y fabricantes que demuestran que cuentan con seguridad, privacidad y confianza incorporadas en el diseño tienen una gran oportunidad para sobresalir de la multitud y de atraer a los consumidores.

CONTRUIR UNA INTERNET DE LAS COSAS CONFIABLE Y SEGURO PARA EL CONSUMIDOR

Esta investigación nos da una idea de lo que los consumidores saben y sienten sobre los aspectos de privacidad y seguridad de los dispositivos conectados, y qué más les gustaría ver para ayudarlos a construir su confianza y disipar sus preocupaciones. Comprender la perspectiva del consumidor y su experiencia de nuevos productos y servicios es crucial para desarrollar intervenciones efectivas de políticas, negocios y defensa.

Estas ideas también contribuirán al trabajo en curso de Consumers International y de Internet Society para crear un entorno de IoT confiable que garantice la seguridad y respete la privacidad, lo que incluye el trabajo en las siguientes áreas:

Fabricantes y comerciantes:

- Una iniciativa de la Internet Society, la **Online Trust Alliance (OTA)** aborda los desafíos en la IoT para crear un mundo conectado más seguro y confiable.
- **Los principios de Confianza por diseño de Consumers International y las pautas que los acompañan** ayudan a los fabricantes a crear dispositivos inteligentes seguros y confiables para los consumidores.
- **Los estándares mínimos para abordar la seguridad de IoT,** por parte de Consumers International, Internet Society y la Fundación Mozilla, lanzaron un conjunto mínimo de requisitos para mantener seguros los dispositivos conectados de los consumidores en el Internet de las cosas.
- **Un llamado conjunto a los comerciantes para que adopten las Pautas de seguridad mínima** y se comprometan a examinar todos los productos conectados que venden según estas pautas de Internet Society, Consumers International, Mozilla y otros socios.

Normas:

- Consumers International es un miembro de enlace de la Organización internacional de normalización que ayuda a desarrollar una nueva norma de protección al consumidor: privacidad por diseño para la norma de bienes y servicios del consumidor (ISO / PC 317) que se centra en productos conectados.

Foros internacionales de formulación de políticas:

- En mayo de 2018, Consumers International fue coanfitrión de la segunda Cumbre de consumidores del G20 en Buenos Aires con un enfoque en la seguridad en línea. Después del evento, la declaración final de los líderes en el G20 solicitó mejoras en la seguridad y la privacidad en la IoT del consumidor, en particular para los productos que se comercializan para los niños.

Conocimiento del consumidor:

- **La campaña Connect-Smart** de Internet Society y Consumers International aumentó la conciencia de los riesgos asociados a los productos conectados que no logran incorporar características básicas de privacidad y seguridad durante la etapa de diseño.

[6] ISO/PC 317 https://www.iso.org/committee/6935430.html
[7] Declaración ministerial sobre la economía digital en el G20. http://www.g20.utoronto.ca/2018/2018-08-24-digital.html

PRÓXIMOS PASOS

> “A PESAR DE QUE EXISTEN GRANDES CANTIDADES DE DISPOSITIVOS CONECTADOS EN LOS HOGARES DE MUCHAS PERSONAS EN LA ACTUALIDAD, PERSISTE LA DESCONFIANZA DEL CONSUMIDOR EN EL IOT.”

Los dispositivos de Internet de las cosas mejoran las actividades diarias de los usuarios de todo el mundo al proporcionar beneficios tales como mayor comodidad, servicios más ágiles y mejor información.

Sin embargo, los resultados de esta encuesta demuestran que persiste la desconfianza del consumidor en el IoT. De hecho, los resultados de la encuesta demuestran que, en algunos casos, esta desconfianza ha desanimado a los consumidores de comprar dispositivos conectados.

Si bien hay muchos factores en juego cuando se trata de la confianza del consumidor en los dispositivos conectados, los fabricantes y comerciantes pueden lograr un impacto significativo al adoptar las normas de seguridad y privacidad de IoT. Al hacerlo, la confianza se integra al diseño y a la venta de dispositivos de IoT; los consumidores pueden comprar y disfrutar de dispositivos IoT más seguros con mayor confianza; y los fabricantes y comerciantes pueden sobresalir aún más como marcas líderes que protegen de forma proactiva los mejores intereses de los consumidores.

> “LOS CONSUMIDORES SE BENEFICIAN CUANDO LA CONFIANZA SE INTEGRA EN EL DISEÑO Y EN LA VENTA DE DISPOSITIVOS DE IOT.”

Internet Society y Consumers International han estado trabajando juntos, y con otros socios, para proporcionar recursos para ayudar a los fabricantes y comerciantes a adoptar las normas de seguridad y privacidad de IoT.

Si usted es un fabricante o comerciante y está interesado en conocer más, puede encontrar más información de la Internet Society en su iniciativa Confianza por diseño o de Consumers International para conseguir una serie de pautas y listas de verificación de IoT.

CONSUMERS INTERNATIONAL

Internet Society

ANEXO
ENCUESTA LLEVADA A CABO POR IPSOS MORI

(Pregunte todo)

P1. Estamos realizando una investigación sobre "dispositivos conectados" en el hogar. Con esto, nos referimos a productos y dispositivos cotidianos que pueden conectarse a Internet (sin incluir tabletas, teléfonos móviles o computadoras portátiles).

¿Cuál (si hubiera) de los siguientes tipos de dispositivos conectados a Internet tiene en su hogar?

Aleatorizar códigos 1-8, código múltiple 1-8.
Los códigos 9, 10 son códigos únicos

1. Aparatos conectados (por ejemplo, medidores de gas/eléctricos, impresoras, altavoces, televisores, refrigeradores, termostatos o limpiadores de pisos robóticos)
2. Portátiles conectados (por ejemplo relojes inteligentes)
3. Monitores de actividad física (por ejemplo Fitbit)
4. Asistentes del hogar (por ejemplo Amazon Alexa o Google Assistant)
5. Consolas de juegos conectadas a internet (por ejemplo, Xbox, PlayStation 4 o Nintendo Wii U)
6. Sistemas de seguridad del hogar conectados (por ejemplo SimplySafe)
7. Juguetes conectados, monitores de bebes o rastreadores GPS para niños (por ejemplo, Hello Barbie, Furby Connect, Phillips Avent, Amber Alert)
8. Automóvil con sistema conectado (por ejemplo, Audi Connect, Lexus Enform, Ford SYNC3)
9. Ninguna de las anteriores
10. No lo sé

.....

(Pregunte todo)

P2. ¿Qué tan probable o improbable es que compre PERSONALMENTE un dispositivo conectado en los próximos 12 meses?

Los dispositivos conectados son productos y dispositivos de uso diario que pueden conectarse a Internet mediante wifi o bluetooth (sin incluir tabletas, teléfonos móviles o computadoras portátiles).

Adelante y atrás escala 1-7, código único

1. Seguro que sí
2. Muy probable
3. Bastante probable
4. Ni probable ni improbable
5. Bastante improbable
6. Muy improbable
7. Seguro que NO
8. No lo sé

.....

(Pregunte si 5 a 7 en P2)

P3. ¿Por qué?

Aleatorizar códigos 1-5, código múltiple 1-5.
El código 6 es un código único

1. No confía en la privacidad o seguridad del dispositivo
2. No tienen ninguna necesidad/uso para ellos.
3. Demasiado caros
4. Realmente no los he considerado
5. No tengo suficiente información sobre qué comprar
6. No hay una razón específica

.....

(Pregunte todo)

P4. Aquí hay una lista de diferentes productos y dispositivos. Para cada uno, ¿qué tan preocupado está (si lo está) acerca de la forma en que recopilan y utilizan los datos personales?

Incluso si no posee los productos o dispositivos, estamos interesados en sus impresiones.

Aleatorizar las afirmaciones (filas), avance/retroceso escala 1-4 (columnas), código único por fila

Columnas

1. Muy preocupado
2. Bastante preocupado
3. No muy preocupado
4. Nada preocupado
5. No lo sé

Filas

1. Teléfonos móviles
2. Tabletas o computadoras portátiles
3. Dispositivos conectados a Internet (como electrodomésticos, asistentes del hogar como Amazon Alexa o Google Assistant, juguetes, monitores de bebes, etc.)
4. Aplicaciones como las que están en los teléfonos inteligentes o tabletas (como los del banco, de salud, etc.)

.....

(Pregunte todo)

P5. Los dispositivos conectados son productos y dispositivos de uso diario que pueden conectarse a Internet mediante wifi o bluetooth (sin incluir tabletas, teléfonos móviles o computadoras portátiles).

En qué medida usted está o no de acuerdo con las siguientes afirmaciones sobre los dispositivos conectados...

Aleatorizar afirmaciones (filas), adelante/atrás escala 1-5 (columnas), código único por fila

Columnas

1. Totalmente de acuerdo
2. Algo de acuerdo
3. Ni de acuerdo ni en desacuerdo
4. Algo en desacuerdo
5. Totalmente en desacuerdo
6. No lo sé

Filas

1. Los dispositivos conectados hacen la vida de las personas más fácil
2. Los dispositivos conectados son perturbadores por la forma en que recopilan datos sobre las personas y sus comportamientos
3. Las personas que no utilizan dispositivos conectados debería probarlos
4. Las personas que utilizan dispositivos conectados deberían estar preocupadas acerca de que sus datos estén siendo utilizados por otras organizaciones sin su permiso
5. Las personas que utilizan dispositivos conectados deberían preocuparse por el riesgo de "escuchas a escondidas" (acceden a los dispositivos sin su conocimiento ni su permiso)

.....

(Pregunte todo)

P6. Los dispositivos conectados son productos y dispositivos de uso diario que pueden conectarse a Internet mediante wifi o bluetooth (sin incluir tabletas, teléfonos móviles o computadoras portátiles).

Cuánto confía (si lo hace) en los dispositivos conectados para...

Aleatorizar las afirmaciones (filas), avance/ retroceso escala 1-4 (columnas), código único por fila

Columnas

1. Mucho
2. Una buena cantidad
3. No mucho
4. Nada
5. No lo sé

Filas

1. ... proteger los datos de los usuarios para que nadie pueda acceder a ellos.
2. ... no ser un riesgo para la privacidad personal de los usuarios.
3. ... garantizar que los datos recopilados sobre los usuarios y sus comportamientos se manejen de manera responsable y transparente
4. ... garantizar que haya suficiente seguridad para permitirle cambiar la configuración de privacidad y seguridad sin afectar el uso

.....

(Pregunte todo)

P6. Los dispositivos conectados son productos y dispositivos de uso diario que pueden conectarse a Internet mediante wifi o bluetooth (sin incluir tabletas, teléfonos móviles o computadoras portátiles).

¿Cómo describiría su conocimiento de las siguientes características de privacidad y seguridad posibles en los dispositivos conectados?

Aleatorizar las afirmaciones (filas), avance/ retroceso escala 1-4 (columnas), código único por fila

Columnas

1. Sí, conocimiento total de esto/cómo hacerlo
2. Sí, conocimiento de esto/cómo hacerlo, pero no en detalle
3. No, no conozco esto/ni de cómo hacerlo
4. Nunca escuché acerca de esto
5. No lo sé

Filas

a) Capacidad de deshabilitar la recopilación de datos de los usuarios y sus comportamientos.

b) Un acuerdo de usuario que explique si los datos son recopilados y si se comparten con un tercero

c) Cifrado para proteger contra el acceso no autorizado a datos sobre los usuarios y sus comportamientos

d) Opción para establecer y restablecer contraseñas

e) Actualizaciones de seguridad automáticas del fabricante

.....

(Pregunte todo)

P7. Los dispositivos conectados son productos y dispositivos de uso diario que pueden conectarse a Internet mediante wifi o bluetooth (sin incluir tabletas, teléfonos móviles o computadoras portátiles).

¿Qué tan importante cree que sería para usted personalmente (si lo es) cada uno de los siguientes factores al tomar una decisión sobre si comprar o no un dispositivo conectado?

Aleatorizar afirmaciones (filas), adelante/ atrás escala 1-5 (columnas), código único por fila

Columnas

1. Muy importante
2. Bastante importante
3. No muy importante
4. Nada importante
5. No lo sé

Filas

1. El dispositivo conectado es fabricado por una marca en la que confío
2. El dispositivo conectado tiene resultados positivos en la prueba del producto o las revisiones en línea
3. El dispositivo conectado lo recomiendan los amigos, la familia o los colegas
4. El dispositivo conectado está a un precio asequible
5. El dispositivo conectado se vende a través de un comerciante en el que confío
6. El dispositivo conectado tiene una etiqueta, adhesivo o marca que certifica que protege la seguridad y es seguro
7. El dispositivo conectado tiene las características que mejor se adaptan a mis necesidades
8. Hay información disponible sobre la privacidad y seguridad del dispositivo conectado, ya sea en un sitio web o en la documentación incluida con el producto (puede ser información del comerciante, fabricante o de una agencia gubernamental de protección al consumidor)

.....

(Pregunte todo)

P8. Los dispositivos conectados son productos y dispositivos de uso diario que pueden conectarse a Internet mediante wifi o bluetooth (sin incluir tabletas, teléfonos móviles o computadoras portátiles).

¿En qué medida usted está o no de acuerdo con las siguientes afirmaciones sobre los dispositivos conectados?

Aleatorizar afirmaciones (filas), adelante/ atrás escala 1-5 (columnas), código único por fila

Columnas

1. Totalmente de acuerdo
2. Algo de acuerdo
3. Ni de acuerdo ni en desacuerdo
4. Algo en desacuerdo
5. Totalmente en desacuerdo
6. No lo sé

Filas

1. Deben existir normas legales de privacidad y seguridad que los fabricantes deben cumplir
2. Los fabricantes sólo deberían producir dispositivos conectados que protejan la privacidad y la seguridad
3. Los comerciantes deberían asegurarse de que los dispositivos conectados que venden tengan buenos estándares de privacidad y seguridad
4. Los consumidores son principalmente responsables de su propia privacidad y seguridad cuando utilizan dispositivos conectados

.....