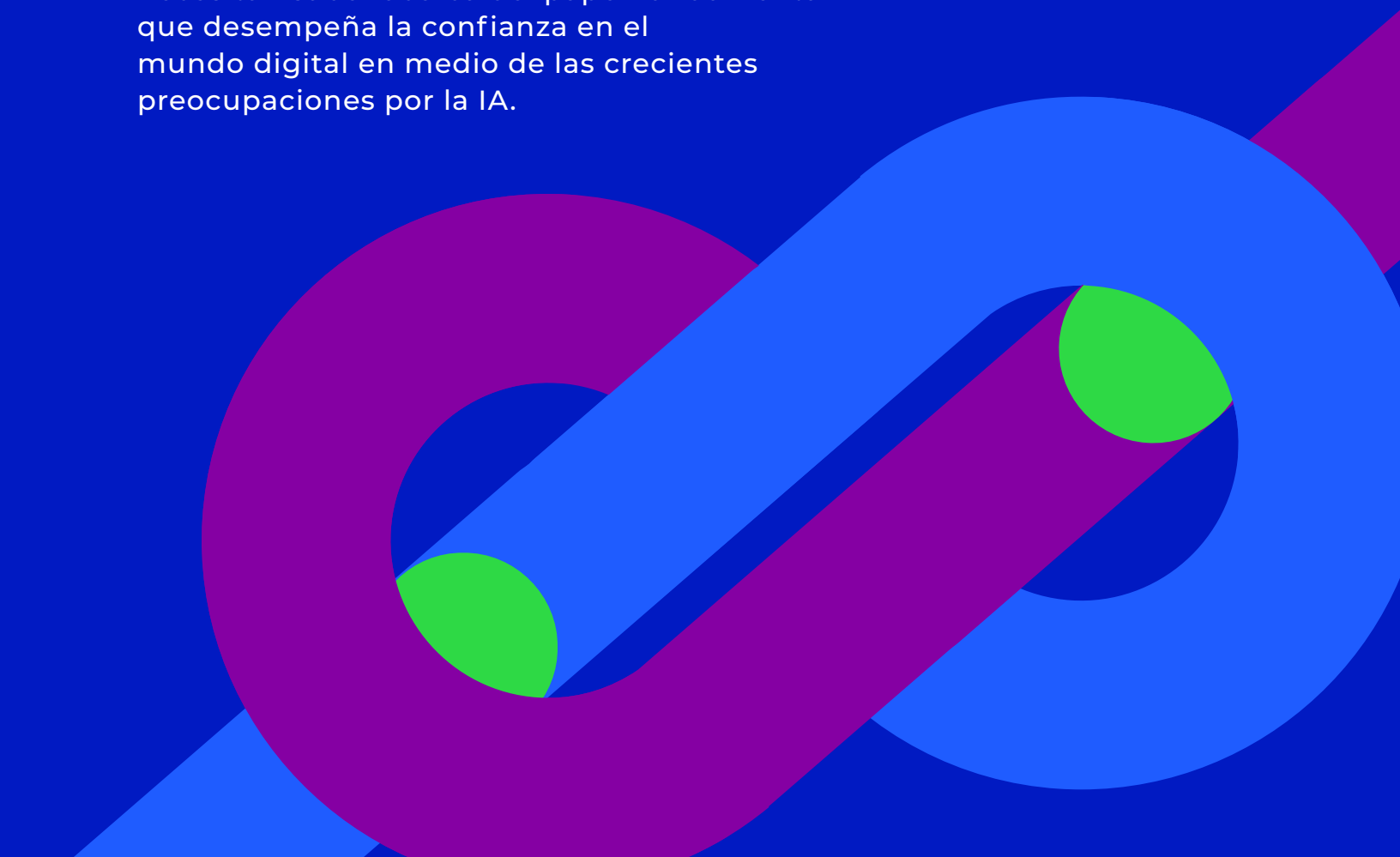
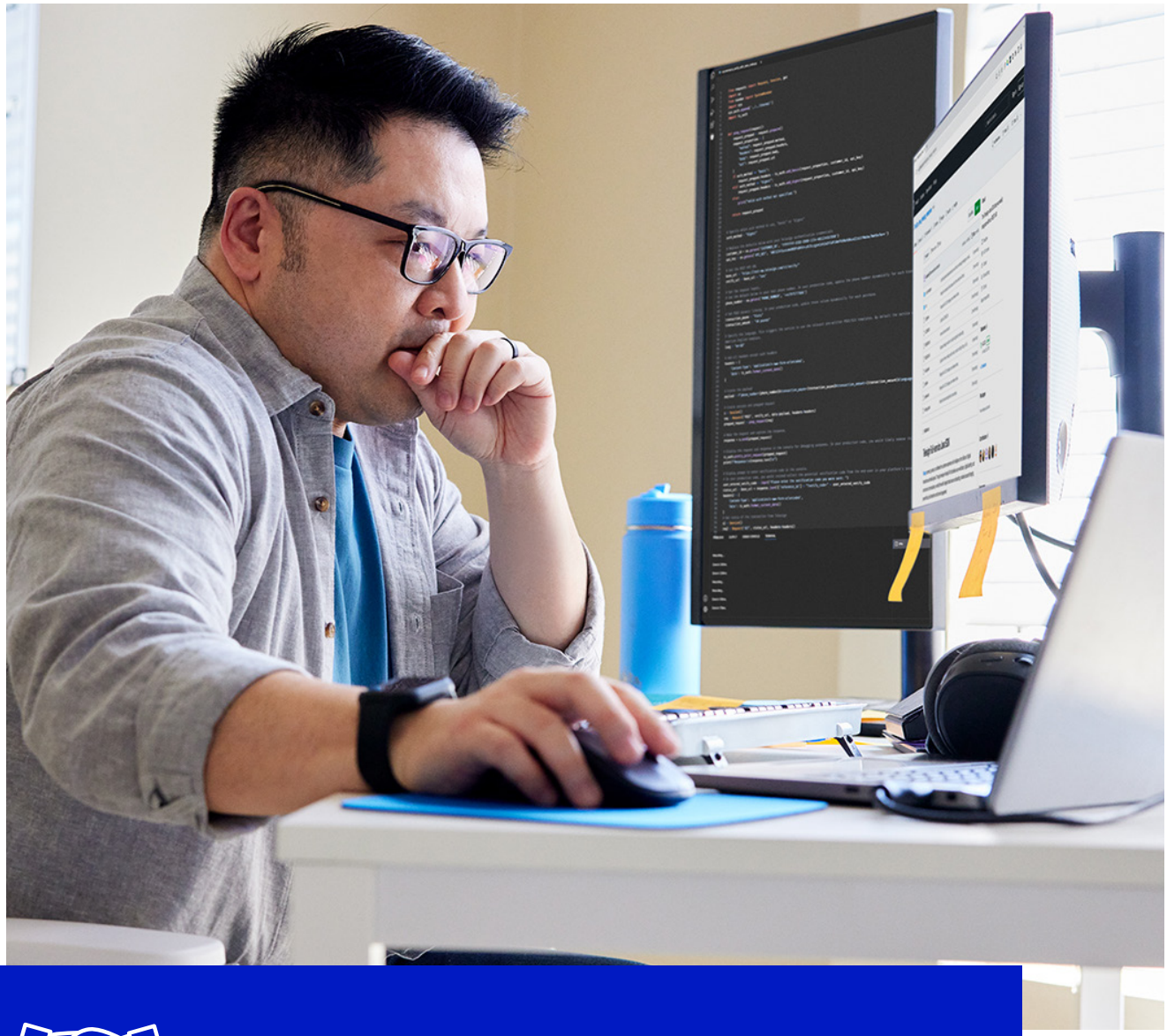
telesign

Trust Index de Telesign 2024

Confianza en la era de la IA

Lo que los líderes globales y las empresas necesitan saber acerca del papel fundamental que desempeña la confianza en el mundo digital en medio de las crecientes preocupaciones por la IA.





La confianza importa, ahora más que nunca.

La irrupción de la IA generativa tiene el potencial de cambiar drásticamente casi todos los aspectos de nuestra vida. El Trust Index de Telesign 2024 muestra cómo el miedo a lo desconocido afecta las percepciones y los comportamientos de los consumidores, y el papel fundamental que tiene la confianza en la exploración del mundo digital.

HALLAZGOS CLAVE

La confianza es fundamental.

El segundo Trust Index anual de Telesign revela cómo la aparición de nuevas tecnologías en el último año está aumentando sustantivamente la importancia de la confianza a nivel mundial en todos los niveles de las empresas y de la sociedad. La toma de conciencia pública de los posibles impactos de la inteligencia artificial (IA) y el aprendizaje automático (ML) sigue siendo confusa; no obstante, con 7 de los 10 países más grandes del mundo yendo a las urnas en 2024, se espera que dicha tendencia cambie enormemente a medida que estas tecnologías emergentes dominen los titulares de los medios de comunicación.

Hallazgos clave de Trust Index 2024

A cuidar la empresa

A pesar del aumento masivo en los intentos de suplantación de identidad o "phishing" y fraudes en línea después del ascenso de la IA generativa, la mayoría de las personas siguen teniendo sentimientos encontrados con relación al impacto que esta tendrá en su susceptibilidad al fraude digital. Esto podría dejar a las personas vulnerables si los servicios con los que interactúan en línea no proporcionan protección contra el fraude digital. Al mismo tiempo, una abrumadora mayoría de las personas cree que las marcas con las que interactúan son responsables de protegerlas del fraude.

Miedo a los "deepfakes"

La mayoría de las personas no cree que haya visto recientemente un video deepfake o una clonación de voz en línea, pero a la gran mayoría le preocupa que la desinformación de los "deepfakes" y las clonaciones de voz afecte negativamente sus elecciones.

Confianza en la votación digital

Aunque la mayoría de las personas preferiría votar en línea si confiara en el sistema de votación, la realidad es que no confían en los sistemas actuales y cuestionarían el resultado de una elección realizada de esta manera.

Aumento del contenido generado por IA

A muchas personas les preocupa que el contenido generado por la IA afecte sus elecciones, y casi la mitad de todas las personas informó que ha visto un anuncio o mensaje político generado por la IA en el último año.

Cómo combatir la IA con la IA

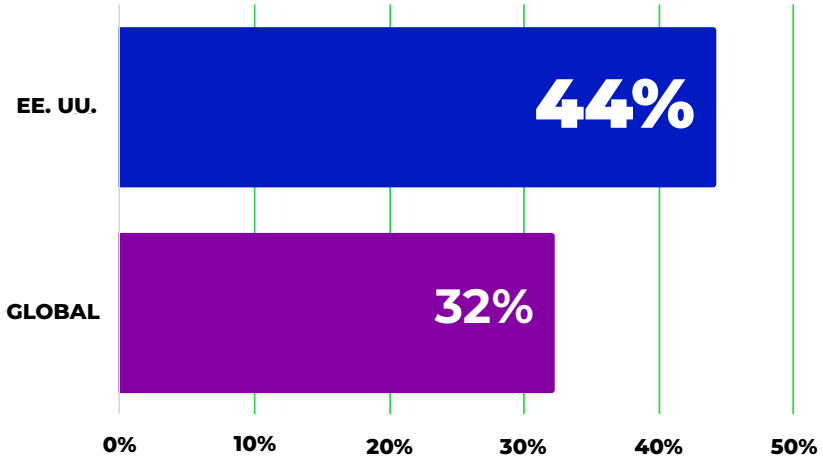
La mayoría de los votantes cree que la desinformación ha hecho que los resultados electorales sean inherentemente menos confiables. También informan que su confianza en el resultado de la elección aumentaría si se utilizara IA o ML para el bien, por ejemplo, para prevenir o detener el fraude, los hackeos y la información falsa. A pesar de que los consumidores valoran la "IA positiva" en el contexto de las elecciones, existe una brecha en su comprensión de cómo los servicios en línea que usan diariamente utilizan la IA y el ML (machine learning) para protegerlos del fraude digital.

PERSPECTIVAS CLAVE

IA Y FRAUDE

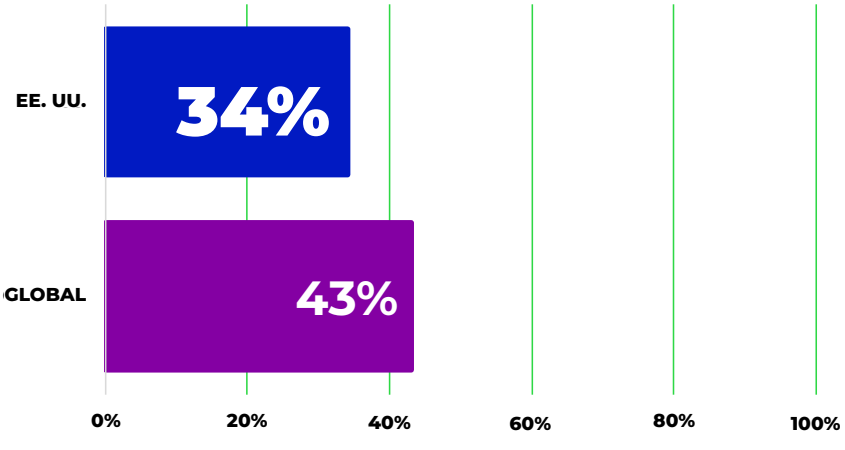
En EE. UU., el 44% de los encuestados cree que la IA/ML no hará diferencia alguna en su susceptibilidad al fraude digital. A nivel mundial, el promedio baja a un 32%.

Casi todos los estadounidenses (un 87%) creen que las empresas con las que interactúan son responsables de proteger la privacidad digital de los usuarios.



Solo el 34% de los encuestados de EE. UU. es más propenso a confiar en una empresa que utiliza IA o ML para protegerse de los ataques de fraude. A nivel mundial, el 43% de los encuestados sigue esta tendencia.

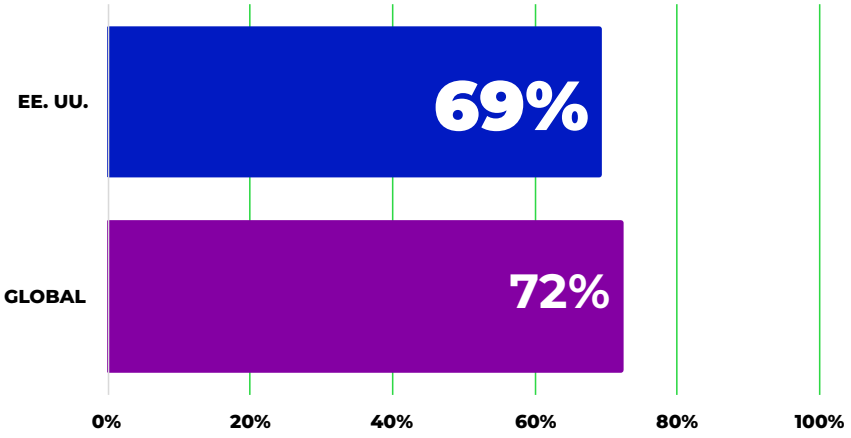
Las personas más jóvenes (un 47%) también son más propensas a confiar en empresas que utilizan IA o ML para proteger de los ataques de los fraudes que las personas mayores (un 39%).



En particular, casi el doble de los brasileños (un 63%) son más propensos a confiar en una empresa que utilice IA o ML para protegerlos de los ataques de fraude.

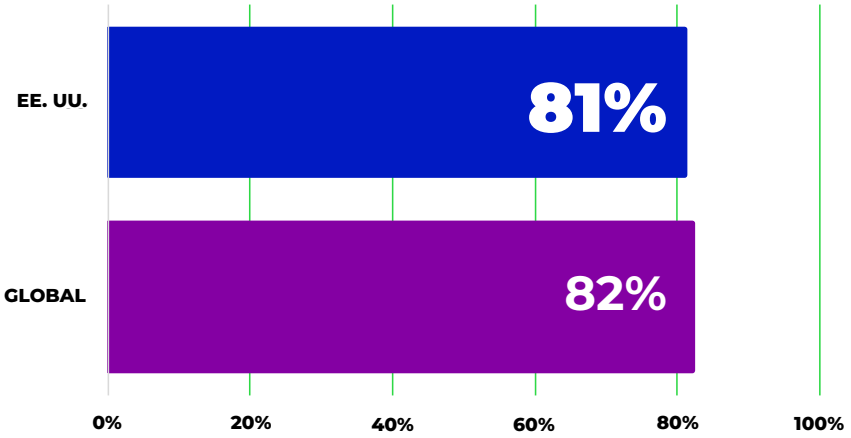
PERSPECTIVAS CLAVE

IA Y "DEEPFAKES"



El 69% de los encuestados en EE. UU. no cree que haya estado expuesto recientemente a videos deepfake o clonaciones de voz. El promedio global aumenta al 72%.

Es más probable que **las víctimas de fraude hayan estado expuestas a un deepfake** o clon en el último año (un 21%).



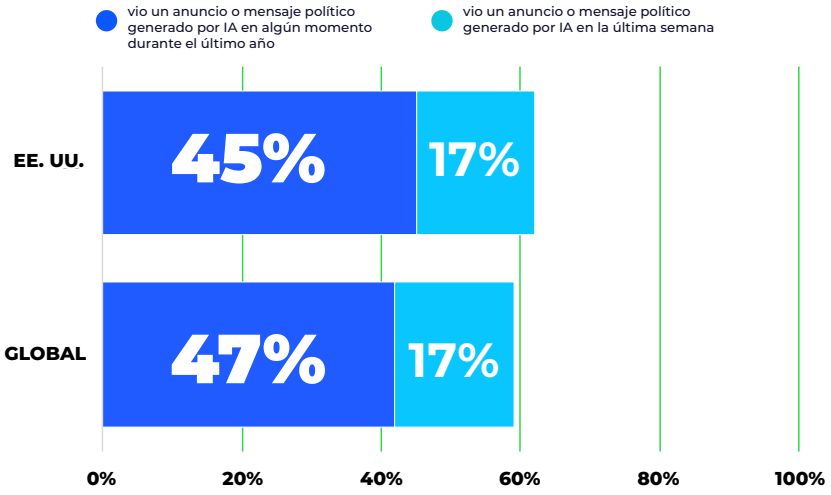
A la gran mayoría de los estadounidenses encuestados (un 81%) le preocupa que la información falsa de los deepfakes y clonaciones de voz afecte negativamente la integridad de sus elecciones. El promedio global es del 82%.

Las personas que se identifican como liberales (un 38%) y conservadoras (un 35%) **están totalmente de acuerdo en que la información falsa afecta de manera negativa las elecciones en** comparación con aquellas personas que se identifican como moderadas (un 28%).

PERSPECTIVAS CLAVE

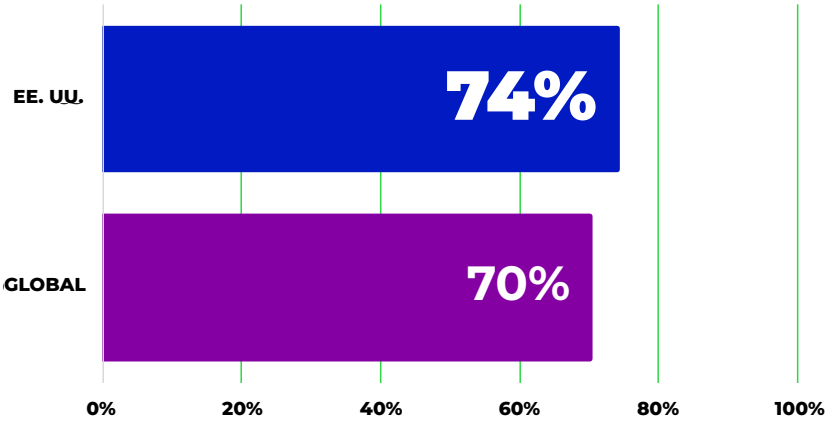
IA Y ELECCIONES

En EE. UU., el 17% de los encuestados informa haber visto un anuncio o mensaje político generado por IA en la última semana, mientras que el 45% ha visto uno en algún momento durante el último año. A nivel mundial, el 17% informa haber visto un anuncio o mensaje político generado por IA en la última semana, mientras que el 47% de las personas ha visto uno en el último año.



Las personas de más de 45 años son mucho más propensas a no estar seguros (un 41%) de si han visto un anuncio o mensaje generado por IA que las que tienen entre 18 y 44 años (un 20%).

El 74% de los encuestados de EE. UU. está de acuerdo en que cuestionaría el resultado de una elección realizada en línea. El promedio global apenas baja al 70%. **Los estadounidenses son los menos propensos a confiar en los resultados de las elecciones en línea.**



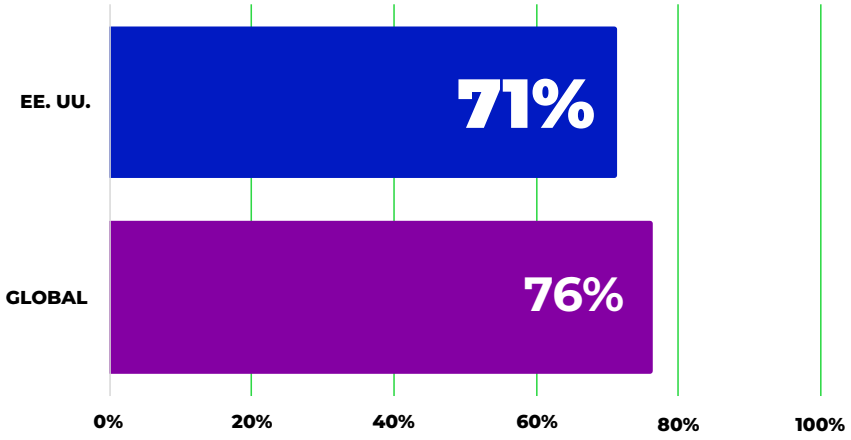
Las personas que se identifican como conservadoras son más propensas (un 76%) a cuestionar el resultado de una elección en línea que aquellas que se identifican como liberales (un 67%) y como moderadas (un 70%).

Al mismo tiempo, el 62% de los estadounidenses preferiría votar en línea si confiara en los sistemas de votación en línea. A nivel mundial, ese número aumenta al 69%, y los estadounidenses muestran el menor nivel de entusiasmo por la votación en línea. Los brasileños y los singapurenses (un 74%) registraron la preferencia más fuerte por la votación en línea.

PERSPECTIVAS CLAVE

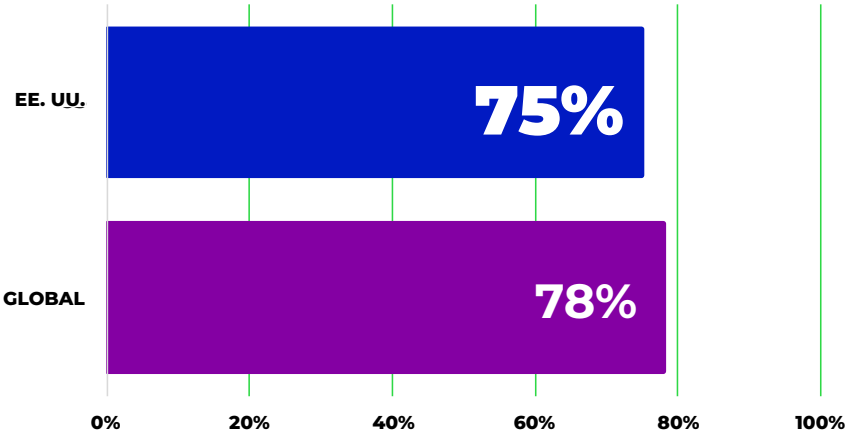
IA Y ELECCIONES

Una gran mayoría de los encuestados estadounidenses (un 71%) presenta una mayor probabilidad de confiar en el resultado de una elección si se utilizara IA y ML para prevenir ciberataques, fraude electoral y hackeos. El promedio global asciende a un 76%.



Mientras tanto, el 83% de los brasileños sería más propenso a **confiar en el resultado de una elección si se utilizara IA y ML para prevenir ciberataques, fraude electoral y hackeos.**

En EE. UU., tres de cada cuatro (un 75%) personas creen que la información falsa ha hecho que los resultados de las elecciones sean inherentemente menos confiables. El promedio global es del 78%.



Siguiendo el mismo criterio, aproximadamente a tres cuartas partes (un 73%) de los estadounidenses **les preocupa que el contenido generado por la IA socave las próximas elecciones,** en línea con el promedio global (un 72%).

Es más probable que las personas conservadoras estén de acuerdo en (un 82%) que la información errónea ha hecho que los resultados electorales sean menos confiables en comparación con las personas que se identifican como liberales (un 72%).

Percepciones clave para las empresas

55%

de las empresas ya están involucradas en al menos una implementación limitada de IA

Las tecnologías digitales están transformando nuestro mundo más rápido de lo que las empresas han sido capaces de transformar su infraestructura digital.

La pandemia por COVID-19 aceleró esta transformación años antes de lo que la mayoría de los expertos creía que sería posible. El debut de ChatGPT y la escalada posterior en el desarrollo de la IA ha acelerado el ritmo de la innovación a una velocidad aún mayor.

Muchas empresas han sido rápidas para reconocer los posibles beneficios económicos de integrar la IA en su infraestructura digital. Según los datos de CompTIA, una voz líder para el ecosistema de TI global, el 55% de las empresas ya están involucradas en al menos una implementación limitada de IA.

También plantea desafíos significativos en cuanto a todas las promesas que mantiene la IA. Los estafadores descubrieron que las herramientas de IA se pueden utilizar para agilizar el fraude y los ciberataques, lo que lleva a un aumento de más del 1,000% en los delitos de suplantación de identidad desde el lanzamiento de ChatGPT.

A medida que el volumen de negocios digitales aumenta año tras año, el potencial de fraude digital mejorado por IA aumenta a la par. La buena noticia: las empresas están tomando nota. Forbes Advisor informa que el 51% de las empresas utiliza IA como ayuda en la gestión de la ciberseguridad y el fraude.

En un futuro cercano, cada empresa tendrá que combatir la IA con la IA.

El segundo Trust Index anual examina el papel central que desempeña la confianza en un mundo configurado por el surgimiento de la IA generativa. Los hallazgos ofrecen información sobre el sentimiento del consumidor respecto de la IA y el ML, y los cambios resultantes en la forma en que las personas interactúan con las empresas y servicios en línea, el contenido que ven en las redes sociales e incluso cómo votan.

El estudio reveló una dicotomía de deseos, en la que los consumidores quieren protección de la IA contra las amenazas existenciales a la democracia y las elecciones, pero se mantienen indecisos acerca de su capacidad de proteger sus datos personales de las amenazas digitales.

El miedo a lo desconocido también surgió como un tema común, lo que presenta una oportunidad para que las empresas no solo adopten las tecnologías de IA y ML, sino también muestren su compromiso de proteger los datos de los clientes. En la era de la IA, las empresas se encuentran ante una encrucijada, con la tarea no solo de adoptar tecnologías innovadoras, sino también de fomentar la confianza. Aquellos que atraviesen este desafío con éxito emergerán como faros de confianza en el mundo digital.

¿Cuáles son las tendencias de fraude digital más recientes que deben conocer las empresas?

Las tácticas de fraude digital evolucionan rápidamente, lo que hace esencial que las empresas se mantengan al día con las estrategias y tendencias de prevención más prevalentes para generar y mantener la confianza del cliente. Algunas tácticas más recientes que utilizan los estafadores para robar a las empresas y sus clientes se enumeran a continuación:

Apropiación de cuentas

La IA generativa ha permitido a los estafadores sobrecargar los ataques de suplantación de identidad. Los datos del **período de 12 meses posterior al lanzamiento de ChatGPT mostraron un aumento del 1265% en los mensajes malintencionados de suplantación de identidad y un aumento del 967% en la suplantación de credenciales.** Ya no hay errores gramaticales ni traducción como había en los mensajes de suplantación de identidad previos a la IA. Con la ayuda de la IA generativa, los estafadores pueden corregir fácilmente estos errores, lo que da como resultado intentos de suplantación de identidad más convincentes y más difíciles de detectar. Y los usan para robar credenciales, apropiarse de cuentas, infiltrarse en empresas y robar datos de clientes. Es fundamental que las empresas utilicen la tecnología para detectar señales de apropiación de cuentas y detenerlas a tiempo.

Cómo aprovechar la MFA

La autenticación multifactor (MFA) estuvo **inactiva en aproximadamente el 99% de las intrusiones digitales exitosas,** de acuerdo con los datos de Microsoft.
A pesar de que la autenticación multifactor ha estado presente desde hace tiempo, muchas empresas aún no la utilizan de manera consistente. La solución es simple, la autenticación multifactor debe activarse de forma predeterminada para proteger la infraestructura digital de cada empresa. La capacitación adecuada del personal de TI y el resto de la empresa también es fundamental para eliminar las intrusiones en la ingeniería social que aprovechan las brechas en la autenticación multifactor.

Cuentas falsas

La proliferación de cuentas falsas también representa una amenaza importante para las empresas que operan en línea. Las personas se escabullen en las comunidades en línea mediante la creación de cuentas falsas, lo que causa estragos entre los usuarios legítimos y, en última instancia, mancha la reputación de la marca.
Un desafío creciente estrechamente asociado con el uso de cuentas falsas es la aparición de deepfakes y clonaciones de voz.

A pesar de que las empresas de tecnología están logrando avances para identificar, etiquetar y eliminar rápidamente imágenes y videos generados por IA del mundo digital, no se presta suficiente atención a cómo se distribuye este contenido. Una de las principales formas es a través de cuentas falsas, en línea y a través de las redes sociales. La mejor manera que tienen las empresas para detener la propagación de cuentas falsas es mejorar los procesos de "conocer a su cliente" (KYC, por sus siglas en inglés) para elevar la vara en la comprobación de si los usuarios son reales.

Metodología

Esta encuesta se realizó en línea y alcanzó un total de n=1,000 finalizaciones en cada mercado. Los encuestados fueron adultos de todas partes de Estados Unidos, Reino Unido, Singapur y Brasil mayores de 18 años. Un subconjunto de los encuestados fueron víctimas de fraude digital en los últimos tres años.

La encuesta se respondió entre el 11 de marzo y el 6 de abril de 2024. El margen de error es de +/- 3,1 puntos porcentuales para cada mercado.

Acerca de Telesign

Telesign proporciona confianza continua (Continuous Trust™) a las principales empresas globales al conectar, proteger y defender sus identidades digitales. Telesign verifica más de cinco mil millones de números de teléfono únicos al mes, lo que representa la mitad de los usuarios de teléfonos celulares del mundo, y brinda información sobre los miles de millones restantes. El potente aprendizaje automático y la amplia ciencia de datos de la empresa brindan recomendaciones de riesgo de identidad con una combinación única de velocidad, precisión y alcance global. Las soluciones de Telesign brindan protección contra fraudes, protegen las comunicaciones y hacen posible la economía digital, ya que ayudan a empresas y clientes interactuar con confianza. Obtén más información en www.telesign.com y síguenos en X, anteriormente conocido como Twitter, en @Telesign.

telesign