

[Anuncios](#)

Los consumidores españoles se relajan en la protección de sus compras online y aumenta el riesgo de ciberataques

- **Los españoles encuestados crearon de media 12 cuentas nuevas durante la pandemia y el 84% reutilizó las contraseñas en todas las cuentas**

- **Un 31% de los encuestados españoles realizaría y pagaría un pedido digitalmente en lugar de ir a una ubicación física o llamar, incluso con preocupaciones sobre la seguridad o privacidad del sitio web o aplicación que estén utilizando**

Cambridge, MA, 15 de junio de 2021 - IBM Security ha anunciado hoy los resultados de una encuesta global que examina los comportamientos digitales de los consumidores durante la pandemia, así como su impacto a largo plazo en la ciberseguridad. Con una sociedad cada vez más acostumbrada a las interacciones digitales, el estudio muestra que las preferencias por la comodidad han superado las preocupaciones por la seguridad y la privacidad entre las personas, lo que ha llevado a tomar malas elecciones en torno a las contraseñas y otros comportamientos de ciberseguridad.

Esta relajación por parte de los consumidores, combinada con la rápida transformación digital de las empresas durante la pandemia, puede aumentar el riesgo de ciberataques en todos los sectores, desde el ransomware hasta el robo de datos. Según IBM Security X-Force, los malos hábitos de seguridad que se llevan a cabo en el plano personal también se trasladan al lugar de trabajo y pueden provocar incidentes de seguridad muy costosos para las empresas, ya que las credenciales de usuario comprometidas fueron una de las principales causas de ciberataques en 2020.

La encuesta global de 22.000 personas en 22 mercados, realizada por Morning Consult para IBM Security, ha identificado los siguientes efectos de la pandemia en los comportamientos de seguridad de los consumidores:

- **El boom digital superará los protocolos de la pandemia** : los españoles crearon 12 nuevas cuentas online de media durante la pandemia. Dado que el 54% no tiene previsto eliminar o desactivar estas nuevas cuentas, los consumidores tendrán una mayor huella digital en los próximos años, lo que ampliará enormemente la superficie de ataque para los ciberdelincuentes.
- **La sobrecarga de cuentas lleva a la fatiga de las contraseñas** : el aumento de las cuentas digitales ha llevado a comportamientos poco rigurosos en cuanto a las contraseñas, ya que el 84% de los encuestados españoles admite que reutiliza las credenciales al menos en algunas ocasiones. Esto significa que la mayoría de las nuevas cuentas creadas durante la pandemia probablemente se basaron en combinaciones reutilizadas de correo electrónico y contraseña, que ya han sido expuestas en brechas de datos en la última década.
- **La comodidad tiene más peso que la seguridad y la privacidad** : casi un tercio (31%) de los

“ Las empresas deben tener en cuenta los efectos de esta dependencia digital en su perfil de riesgo de seguridad. Con las contraseñas cada vez menos fiables, una forma en que las organizaciones pueden adaptarse, más allá de la autenticación multifactor, es cambiar a un enfoque de "confianza cero", aplicando IA y análisis avanzados en todo el proceso para detectar posibles amenazas, en lugar de asumir que un usuario es de confianza después de la autenticación ”

encuestados españoles preferiría hacer un pedido y pagarlo utilizando una aplicación o un sitio web potencialmente inseguro en lugar de llamar o ir a un lugar físico en persona. Dado que los usuarios son más propensos a pasar por alto las preocupaciones de seguridad por la comodidad de los pedidos digitales, la carga de la seguridad recaerá más en las empresas que prestan estos servicios para evitar el fraude.

- **Aceleración de la telesalud y la identificación digital:** a medida que los consumidores se inclinan más hacia las interacciones digitales, estos comportamientos también tienen el potencial de estimular la adopción de tecnologías emergentes en una variedad de entornos, desde la telesalud hasta la identidad digital.

"Las empresas deben tener en cuenta los efectos de esta dependencia digital en su perfil de riesgo de seguridad. Con las contraseñas cada vez menos fiables, una forma en que las organizaciones pueden adaptarse, más allá de la autenticación multifactor, es cambiar a un enfoque de "confianza cero", aplicando IA y análisis avanzados en todo el proceso para detectar posibles amenazas, en lugar de asumir que un usuario es de confianza después de la autenticación", ha señalado Charles Henderson, socio director global y jefe de IBM Security X-Force

Los consumidores tienen grandes expectativas sobre la facilidad de acceso y uso

La encuesta también revela los hábitos de los consumidores en sus interacciones digitales. En este contexto, dos tercios (67%) de los españoles encuestados esperan pasar menos de 5 minutos configurando una nueva cuenta digital. Además, en España, los usuarios intentan iniciar sesión como máximo 3 veces antes de restablecer su contraseña. Estos restablecimientos no sólo cuestan dinero a las empresas, sino que también pueden suponer una amenaza para la seguridad si se utilizan en combinación con una cuenta de correo electrónico ya comprometida.

Por otra parte, aunque la reutilización de contraseñas es un problema creciente, añadir un factor adicional de verificación para las transacciones de mayor riesgo puede ayudar a reducir el riesgo de que la cuenta se vea comprometida. La encuesta señala que más de un 70% de los españoles utilizan frecuentemente la autenticación multifactor.

Preparando el camino para las credenciales digitales

El concepto de tarjetas sanitarias digitales o los pasaportes de vacunación son un caso de uso real de las credenciales digitales, que ofrecen un enfoque basado en la tecnología para verificar aspectos específicos de nuestra identidad. Según la encuesta, el 59% de españoles encuestados dicen estar familiarizados con el concepto de credenciales digitales, y el 73% estaría dispuesto a adoptarlas si fueran comúnmente aceptadas.

Si bien el aprovechamiento de una forma digital de identidad también puede crear un modelo de seguridad y privacidad más sostenible para el futuro, deben establecerse protecciones de seguridad para evitar la falsificación, lo que exige las capacidades de las soluciones de blockchain para verificar y proporcionar la capacidad de actualizar estas credenciales en caso de que se vean comprometidas.

Cómo pueden adaptarse las organizaciones al cambiante panorama de la seguridad de los consumidores

Las empresas que se han vuelto cada vez más dependientes del compromiso digital con los consumidores como resultado de la pandemia deben considerar el impacto que esto tiene en sus perfiles de riesgo de ciberseguridad. A la luz de los cambios en los comportamientos y preferencias de los consumidores en torno a la comodidad digital, IBM Security ofrece la siguiente orientación:

- **Enfoque de confianza cero:** este método opera bajo el supuesto de que una identidad autenticada, o la propia red, puede estar ya comprometida, y por lo tanto valida continuamente las condiciones de conexión entre usuarios, datos y recursos para determinar la autorización y la necesidad. Este enfoque requiere que las empresas unifiquen sus datos y enfoque de seguridad, con el objetivo de envolver el contexto de seguridad alrededor de cada usuario, cada dispositivo y cada interacción.
- **Modernización de la IAM del consumidor:** Invertir en una estrategia modernizada de Gestión de Identidades y Accesos de los Consumidores (CIAM) puede ayudar a las empresas a aumentar el compromiso digital, proporcionando una experiencia de usuario sin fricciones a través de las plataformas digitales y utilizando el análisis del comportamiento para disminuir el riesgo de uso fraudulento de las cuentas.
- **Protección de datos y privacidad:** las organizaciones deben asegurarse de que existen controles fuertes de seguridad de los datos para evitar el acceso no autorizado, desde la supervisión de los datos para detectar actividades sospechosas, hasta el cifrado de los datos sensibles dondequiera que viajen. Las empresas también deben aplicar las políticas de privacidad adecuadas en sus instalaciones y en la nube para mantener la confianza de los consumidores.
- **Ponga la seguridad a prueba:** las empresas deben considerar la posibilidad de realizar pruebas específicas para garantizar que las estrategias y tecnologías de seguridad en las que han confiado anteriormente siguen siendo válidas. Reevaluar la eficacia de los planes de respuesta a incidentes y probar las aplicaciones para detectar vulnerabilidades de seguridad son componentes importantes de este proceso.

Para ver el informe completo y los recursos: http://ibm.biz/IBMSecurity_ConsumerSurvey

Acerca de IBM Security

IBM Security ofrece una de las carteras más avanzadas e integradas de productos y servicios de seguridad empresarial. Esta cartera, respaldada por la mundialmente conocida investigación IBM Security X-Force®, permite a las organizaciones gestionar eficazmente los riesgos y defenderse de las amenazas emergentes. IBM cuenta con una de las organizaciones de investigación, desarrollo y suministro de seguridad más amplias del mundo, supervisa más de 150.000 millones de eventos de seguridad al día en más de 130 países y ha obtenido más de 10.000 patentes de seguridad en todo el mundo. Para más información, consulte www.ibm.com/security, siga a @IBMSecurity en Twitter o visite el blog de IBM Security Intelligence.

Metodología del informe: En marzo de 2021, Morning Consult realizó una encuesta mundial en nombre de IBM. El estudio se realizó entre 22.000 adultos en 22 mercados (1.000 encuestados por mercado), incluyendo Alemania, Argentina, Australia, Brasil, Canadá, Chile, Colombia, Corea del Sur, España, Estados Unidos, Francia, India, Italia, Japón, México, Perú, Singapur, Reino Unido, Oriente Medio, Europa Central y del Este, Países Nórdicos y BNL (Bélgica, Países Bajos y Luxemburgo).

For further information: Patricia Núñez IBM Comunicación patricia.nunez@es.ibm.com
