**NOTICIAS SOBRE CIBERSERGURIDAD**

|  |  |
| --- | --- |
| Sextorsión en auge | <https://cybersecuritynews.es/sextorsion-en-auge-ciberdelincuentes-exigen-pagos-en-bitcoines-amenazando-con-difundir-videos-intimos/> |
| La aseguradora de salud estadounidense Centene | <https://www.bbc.com/news/technology-35420306> |
| Neiman Marcus dice que los piratas informáticos violaron las cuentas de los clientes | <https://www.securityweek.com/neiman-marcus-says-hackers-breached-customer-accounts/> |
| El Gran Golpe de Musk: ¿Twitter sepultado por Capricho o Estrategia? | <https://news.america-digital.com/el-gran-golpe-de-musk-twitter-sepultado-por-capricho-o-estrategia/> |
| Telefónica Tech refuerza 'The ThinX', su laboratorio de tecnología IoT y 'big data | <https://www.europapress.es/economia/noticia-telefonica-tech-refuerza-the-thinx-laboratorio-tecnologia-iot-big-data-20230628112312.html> |

1. **Sextorsión en auge**

**Who: Instituto Nacional de Ciberseguridad de España**

**What: Una campaña de sextorsión a través de correos electrónicos fraudulentos que buscan extorsionar a sus víctimas al afirmar que poseen grabaciones íntimas y amenazan con compartirlas con los contactos de la víctima si no se realiza un pago en bitcoines en un plazo de 48 horas.**

**When: La campaña ha sido identificada en "los últimos días".**

**Where: La campaña se lleva a cabo a través de correo electrónico y puede afectar a cualquier persona que reciba los correos electrónicos fraudulentos.**

**Why: Los extorsionadores utilizan la sextorsión como un método para extorsionar dinero de sus víctimas aprovechando el miedo y la vergüenza**

El Instituto Nacional de Ciberseguridad (INCIBE) ha emitido una alerta sobre una nueva campaña de correos electrónicos fraudulentos que emplea la sextorsión como método de extorsión. Los estafadores envían correos desde cuentas generadas al azar con asuntos llamativos, afirmando tener videos íntimos comprometedores de la víctima. Amenazan con compartir estos videos con los contactos de la víctima a menos que se realice un pago en bitcoins en 48 horas.

Los extorsionadores afirman que el dispositivo de la víctima está infectado con un software espía indetectable por los antivirus, y que ha capturado los videos comprometedores. La víctima es presionada para pagar rápidamente debido al corto plazo de 48 horas y a la amenaza de difundir el material comprometedor.

Las autoridades advierten a los usuarios que no deben realizar ningún pago y que eliminen los correos sospechosos. No se debe responder al extorsionador, ya que esto podría indicar que la cuenta está activa y llevar a futuros fraudes. Si alguien ha sido víctima de la extorsión y ha realizado el pago, se recomienda recopilar pruebas y presentar una denuncia a las autoridades. También se sugiere buscar testigos en línea y ejercer el derecho al olvido para eliminar información perjudicial.

La prevención es esencial para evitar este tipo de ataques. Se recomienda mantener actualizado el software antivirus, evitar sitios web sospechosos y mantener la calma ante amenazas o solicitudes de pago inesperadas.

1. **La aseguradora de salud estadounidense Centene**

**Who: La compañía de seguros de salud Centene Corporation**

**What: Casi un millón de registros médicos de personas han desaparecido debido a la pérdida de seis discos duros que contenían información personal y de salud de los clientes de Centene entre 2009 y 2015.**

**When: la pérdida de datos ocurrió en algún momento entre 2009 y 2015**

**Where: El incidente ocurrió en Centene Corporation, una compañía de seguros de salud de EE. UU.**

**Why: La pérdida de los registros médicos ocurrió debido a la desaparición de seis discos duros que contenían información personal y de salud de los clientes de la compañía.**

La compañía de seguros de salud Centene Corporation admitió que los registros médicos de casi un millón de personas habían desaparecido. Los registros se almacenaban en seis discos duros internos que contenían información personal y de salud de los clientes. Estos registros incluían nombres, direcciones, fechas de nacimiento, números de seguro social, detalles de membresía e información de salud de los clientes. Aunque no se incluían detalles financieros o de pago en las unidades.

La información en los discos duros pertenecía a alrededor de 950,000 personas que habían recibido servicios de laboratorio entre 2009 y 2015. Centene afirmó que estaba realizando una búsqueda interna para localizar los discos duros.

Aunque no se creía que la información se hubiera utilizado de manera inapropiada, la compañía decidió tomar medidas de precaución y transparencia al revelar la pérdida y llevar a cabo una búsqueda continua de los discos duros.

La empresa prometió notificar a los afectados y ofrecerles seguimiento médico gratuito. También mencionó que reforzaría y revisaría sus procedimientos para prevenir incidentes similares en el futuro.

La situación tiene implicaciones importantes ya que Centene maneja información de salud confidencial de sus miembros. Los expertos legales opinaron que la compañía probablemente tendría que presentar un informe a las autoridades reguladoras de EE. UU. y podría enfrentar multas por la pérdida de datos.

En el pasado, ha habido casos similares de pérdida o robo de registros médicos, algunos de los cuales resultaron en ataques cibernéticos o robos de datos masivos que afectaron a cientos de miles o incluso millones de personas. Tales incidentes pueden tener graves consecuencias para la seguridad y privacidad de los individuos cuyos datos se ven comprometidos.

1. **Neiman Marcus dice que los piratas informáticos violaron las cuentas de los clientes**

**Who: El minorista de lujo Neiman Marcus Group y sus clientes afectados por el ataque cibernético.**

**What: Los ciberdelincuentes llevaron a cabo un ataque automatizado para probar varias combinaciones de nombre de usuario y contraseña en los sitios web de Neiman Marcus**

**When: El ataque comenzó alrededor del 26 de diciembre**

**Where: El ataque afectó a los sitios web de Neiman Marcus, Last Call, Bergdorf Goodman, Horchow y CUSP.**

**Why: Los ciberdelincuentes llevaron a cabo el ataque para obtener acceso a las cuentas de los clientes y posiblemente realizar compras no autorizadas en los sitios web.**

El minorista de lujo Neiman Marcus Group sufrió un ataque cibernético en el que piratas informáticos intentaron acceder a las cuentas en línea de sus clientes. Los hackers utilizaron un ataque automatizado para probar diferentes combinaciones de nombre de usuario y contraseña en los sitios web de Neiman Marcus y sus marcas relacionadas. El ataque ocurrió a partir del 26 de diciembre.

Aproximadamente 5200 cuentas fueron comprometidas, pero no se robaron las combinaciones de nombre de usuario y contraseña de los sistemas de la empresa. En cambio, se cree que los atacantes utilizaron credenciales robadas de otras organizaciones para intentar acceder a las cuentas de los clientes de Neiman Marcus, sabiendo que muchas personas reutilizan contraseñas.

A pesar del ataque, Neiman Marcus afirmó que más del 99% de los intentos fueron repelidos por sus defensas cibernéticas. Los atacantes lograron realizar compras no autorizadas utilizando alrededor de 70 de las cuentas comprometidas, pero el equipo antifraude del minorista detectó estas compras y reembolsó a los clientes afectados.

Las cuentas comprometidas contenían información como nombres de clientes, información de contacto, últimos cuatro dígitos de números de tarjetas de pago y historial de compras. Sin embargo, datos más sensibles como números de seguro social, fechas de nacimiento, números completos de cuentas bancarias y PIN no estaban en riesgo.

Neiman Marcus anunció que requerirá a todos los clientes afectados que cambien sus contraseñas la próxima vez que inicien sesión. La empresa también destacó que sus medidas de defensa funcionaron en gran medida como se esperaba durante el ataque.

Este no fue el primer incidente de seguridad que enfrentó Neiman Marcus, ya que en 2014 también sufrió un ataque en el que se robaron datos de tarjetas de pago de clientes utilizando malware de punto de venta. En ese momento, se reveló que hasta 1,1 millones de tarjetas podrían haber sido comprometidas, pero la cifra final fue menor, afectando a aproximadamente 350,000 tarjetas.

1. **El Gran Golpe de Musk: ¿Twitter sepultado por Capricho o Estrategia?**

**Who: Elon Musk, el CEO de Tesla y propietario de Twitter, y los usuarios de la plataforma.**

**What: Elon Musk ha cambiado el logotipo de Twitter, reemplazando el icónico pájaro azul por una X en blanco y negro. Además, ha insinuado un posible cambio de nombre de la plataforma a "X" y una transformación total de la plataforma para abarcar comunicación, multimedia y un sistema financiero único, ofreciendo de esta manera una mayor seguridad en la plataforma.**

**When: Elon Musk insinuó el cambio a través de tweets, y el cambio de logotipo ocurrió poco después de publicar una imagen con el logo X proyectado en la sede de la empresa.**

**Where: El cambio de logotipo y las insinuaciones de cambios de seguridad en la plataforma ocurrieron en Twitter, una plataforma de redes sociales.**

**Why: Elon Musk ha expresado su visión de transformar Twitter en una plataforma más amplia, versátil y más segura que abarque comunicación, multimedia y servicios financieros, como una súper aplicación similar a WeChat en China.**

Elon Musk ha llevado a cabo su promesa de cambiar el logotipo de Twitter y transformar la plataforma. ¿Inicialmente, insinuó el cambio en una serie de tweets que simplemente decían “x?". Luego, confirmó que Twitter cambiaría su marca a "X" y eliminaría gradualmente el icónico pájaro azul.

El lunes, Musk publicó una imagen proyectando el nuevo logo "X" en la sede de la empresa, lo que marcó el cambio oficial en la plataforma. También insinuó cambios en el término "retweets" y en el color de la plataforma, sugiriendo que todo el concepto debería ser repensado.

La nueva directora ejecutiva de Twitter, Linda Yaccarino, respaldó este cambio, afirmando que "X" será la plataforma que ofrecerá una interactividad ilimitada centrada en audio, video, mensajería, pagos/banca y creará un mercado global para ideas, bienes y servicios.

El objetivo de Musk con este cambio es crear sinergias entre Twitter y su antigua empresa, X.com, ofreciendo una plataforma que abarque comunicación, multimedia y funciones financieras más seguras en una sola aplicación. También se menciona la posibilidad de incluir características bancarias y de pago similares a la aplicación china WeChat.

A pesar de los obstáculos y críticas, Musk está decidido a transformar tanto las redes sociales como las transacciones financieras. Su visión de "X" se basa en su pasado, ya que en la década de 1990 fundó X.com, una plataforma de servicios financieros y banca en línea. Aunque dejó la empresa, este concepto influyó en su visión actual.

El cambio a "X" ha atraído la atención mundial nuevamente hacia la plataforma, lo que es fundamental para recuperar su valor de marca perdido debido a la competencia y la disminución de los ingresos por publicidad.

En resumen, Elon Musk ha transformado Twitter cambiando su logotipo a "X" y aspirando a crear una plataforma que revolucione tanto las redes sociales como las transacciones financieras. Su visión de "X" se basa en su experiencia pasada y su deseo de promover la interacción humana única. Aunque enfrenta obstáculos, Musk está decidido a lograr su visión de futuro.

1. **Telefónica Tech refuerza 'The ThinX', su laboratorio de tecnología IoT y 'Big Data**

**Who: Telefónica Tech, una empresa de tecnología y telecomunicaciones**

**What: Telefónica Tech ha inaugurado un nuevo laboratorio llamado 'The ThinX', enfocado en tecnología IoT (internet de las cosas) y 'Big Data'.**

**When: La inauguración del laboratorio 'The ThinX' ocurrió en 2023.**

**Where: El laboratorio 'The ThinX' está ubicado en Madrid, España.**

**Why: El objetivo del laboratorio es anticiparse a la creciente demanda de servicios relacionados con IoT y 'Big Data', así como ayudar a los clientes en su transformación digital.**Telefónica Tech ha inaugurado en Madrid un nuevo laboratorio llamado 'The ThinX', como parte de su Hub Mundial de Innovación y Talento establecido en 2021. El objetivo principal de este laboratorio es estar preparados para la creciente demanda de servicios relacionados con el Internet de las Cosas (IoT) y el análisis de grandes datos ('big data'). La iniciativa tiene como propósito ayudar a los clientes en su proceso de transformación digital. Puedes obtener más detalles en el enlace proporcionado.

**¿Qué información tienen en común cada una de las noticias?**

Los cinco casos han sido víctimas de ciberdelincuencia.

A partir de unos fallos de seguridad, como, por ejemplo, abrir enlaces dudosos, perdida de almacenamiento físico de datos o los ataques cibernéticos, muestran la debilidad de la red en el caso de no seguir unos procedimientos de seguridad básicos.

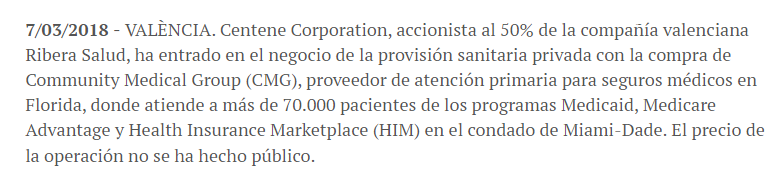
**Búsqueda e identificación de la fuente original de la noticia**

**Sextorsión en auge**



**La aseguradora de salud estadounidense Centene**





**Neiman Marcus dice que los piratas informáticos violaron las cuentas de los clientes**



**El Gran Golpe de Musk: ¿Twitter sepultado por Capricho o Estrategia?**



**Telefónica Tech refuerza 'The ThinX', su laboratorio de tecnología IoT y 'Big Data**

****

****