RESOURCE CENTER

Mes de concienciación sobre la ciberseguridad

Get the full interactive view at
https://bitwarden.com/es-la/resources/cybersecurity-awareness-month/

bitwarden

Ciberseguridad sencilla: 4 pasos para la seguridad en línea

Índice

> "El Mes de Concienciación sobre la Ciberseguridad, que se celebra cada octubre, es una colaboración entre el gobierno y la industria privada para concienciar sobre la seguridad digital y capacitar a todo el mundo para proteger sus datos personales de las formas digitales de delincuencia."

- Alianza Nacional de Ciberseguridad

Primer paso. Las contraseñas fuertes y únicas sientan las bases de la ciberseguridad

A diario, la persona media se conecta a alguna variación de Instagram, TikTok, aplicaciones bancarias, cuentas de trabajo, correo electrónico personal, sitios de comercio electrónico y cuentas de viajes compartidos. Es justo decir que vivimos en un mundo en línea.

Cuando los usuarios comparten tanta información, ¿cómo pueden mantenerse seguros? En realidad es sencillo. Utilizar contraseñas fuertes y únicas ayuda a proteger tus datos. ¿No está seguro de si sus contraseñas son lo suficientemente seguras? Pon a prueba su seguridad y aprende más sobre la gestión de contraseñas. También puedes empezar ahora con una cuenta gratuita con todas las funciones para un número ilimitado de inicios de sesión en un número ilimitado de dispositivos.

"70% of people admit they use the same password for more than one account."

PC Mag

https://player.vimeo.com/video/752654111

Segundo paso. Utilice la autenticación multifactor

La autenticación de dos factores (2FA), el inicio de sesión en dos pasos o la autenticación multifactor (MFA) hacen referencia a los distintos métodos de verificación de la identidad para acceder a una cuenta. Esto puede incluir iniciar sesión en una cuenta con una contraseña y luego volver a confirmar con un código de autenticación. Para una explicación más detallada, consulta este post sobre las 10 preguntas más candentes sobre 2FA y para más información sobre los diferentes métodos de 2FA/MFA, visita este artículo de ayuda sobre el inicio de sesión en dos pasos. En pocas palabras, el inicio de sesión en dos pasos ofrece la capa adicional de protección que todo el mundo necesita.

Did you know?

Passkey 2FA is included in every Bitwarden plan, including free! All users can secure their Bitwarden account with a hardware security key or other FIDO2 WebAuthn credential generator.

https://player.vimeo.com/video/752706739

Visite The Survey Room: una colección de encuestas e informes relacionados con la gestión de contraseñas y la seguridad que abarcan a empresas y particulares.

Paso 3. Mantenga actualizado su software

El Mes de la Concienciación sobre la Ciberseguridad nos recuerda a todos que debemos estar al tanto de las actualizaciones de software. Normalmente, las actualizaciones parchean fallos de seguridad, eliminan errores y añaden funciones que pueden proteger mejor la información. Aunque es tentador renunciar a las actualizaciones, un par de minutos de actualizaciones podrían evitar horas de dolores de cabeza derivados de una identidad robada.

Las actualizaciones de software también ayudan a prevenir los ataques de ransomware. Normalmente, los ciberdelincuentes centrados en los rescates intentan aprovecharse de las vulnerabilidades, incluidas las del software obsoleto.

66% of respondents reported their organization was affected by ransomware in 2023, up from 51% in 2020.

2023 Sophos State of Ransomware Report

https://player.vimeo.com/video/752707997

Paso 4. Sepa cómo detectar una estafa de phishing

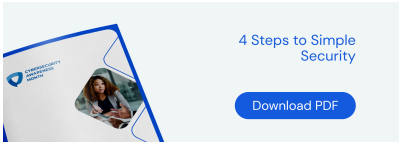
Aprenda a mantenerse alerta ante los ataques de phishing, que se refieren al intento de engañar a las personas para que compartan datos valiosos o visiten sitios web infectados con malware. Los usuarios deben comprobar que los correos electrónicos proceden del remitente correcto, pasar el ratón por encima de los enlaces para confirmar que van al sitio web adecuado y evitar abrir archivos adjuntos de personas que no conocen. Tenga especial cuidado en los dispositivos móviles, que no siempre disponen de la opción de pasar el ratón por encima para ver la dirección de correo electrónico exacta y los destinos de los enlaces.

Además, herramientas como los gestores de contraseñas pueden ayudar. Más información sobre cómo los gestores de contraseñas ayudan a prevenir el phishing.

https://player.vimeo.com/video/752708367

Recursos adicionales

- 7 pasos para crear un perfil seguro y privado en Internet
- La sala de encuestas
- Por qué las empresas necesitan un gestor de contraseñas
- Qué significa para las empresas la adopción de la tecnología sin contraseña
- Cómo optar a un ciberseguro con una gestión segura de contraseñas
- Ventajas de ofrecer la gestión de contraseñas como servicio
- Acelerar el valor para los usuarios de Bitwarden - Bitwarden recauda 100 millones de dólares
- Conozca la opinión de los expertos sobre Bitwarden



Únase a nosotros en este Mes de Concienciación sobre la Ciberseguridad para varios Twitter Spaces con el equipo de Bitwarden sobre algunos temas interesantes de ciberseguridad. Síganos en Twitter para no perderse la diversión.