

Mes de la Concientización sobre la Ciberseguridad 2024 **Ejemplos de publicaciones en redes sociales**

Etiquetas oficiales: #CybersecurityAwarenessMonth #SecureOurWorld

Utilice estas publicaciones en sus plataformas de redes sociales durante el Mes de Concientización sobre la Ciberseguridad.

Puede copiarlas y pegarlas, o modificar el texto para que se adapte mejor a su campaña. Enlace a sus propios recursos y sitios web o a estas páginas oficiales de la campaña del Mes de Concientización sobre la Ciberseguridad:

<https://www.cisa.gov/cybersecurity-awareness-month>

<https://staysafeonline.org/programs/cybersecurity-awareness-month/>

Campaña

1. ¡Octubre es el #CybersecurityAwarenessMonth! Hay muchas formas diferentes de mantenerse seguro en línea. Obtén más información sobre lo que puedes hacer para ayudar #SecureOurWorld.
2. ¡Feliz #CybersecurityAwarenessMonth! ¿Qué medidas has tomado hasta ahora para mantenerte seguro en línea y #SecureOurWorld? Marca esas casillas de tu lista y encuentra más recursos aquí.
3. ¿Intento de phishing? Denunciado. ¿Software? Actualizado. ¿Autenticación multifactor? Activada. ¿Contraseñas? Seguras y herméticas. Estamos listos para el #CybersecurityAwarenessMonth #SecureOurWorld
4. Ha llegado el momento del año para ayudar a la abuela a actualizar su enrutador y avisarles a tus amigos de Facebook que no acepten la solicitud del "nuevo" perfil de tu amigo. Obtén más información sobre #CybersecurityAwarenessMonth y como puedes #SecureOurWorld.
5. ¿Has hablado con tu #familia sobre la seguridad en línea? Los #Cyberattacks están en aumento, así que habla con tus hijos, tus padres y tu comunidad sobre cómo mantenerse seguro en línea y #SecureOurWorld. #fraudeamayores #robodeidentidad #phishing

Ciberseguridad.

6. La ciberseguridad significa "¡no toques mis cosas!" Obtén más información sobre por qué es importante mantener tus cosas como tuyas: (enlace) #CybersecurityAwarenessMonth #SecureOurWorld
7. En la era de la tecnología, la ciberseguridad nunca ha sido más importante. Si bien esto puede parecer obvio, algunas de las grietas en tu armadura podrían no serlo. Aprovecha esta oportunidad este #CybersecurityAwarenessMonth para volver a comprobar tus protecciones digitales. #SecureOurWorld

8. En un mundo cada vez más digital, es importante mantener la ciberseguridad como una prioridad. Mantente seguro en línea y ayuda a #SecureOurWorld este #CybersecurityAwarenessMonth.
9. A medida que la inteligencia artificial (AI, por sus siglas en inglés) se vuelve más sofisticada y los deepfakes más realistas, debemos ser más inteligentes en materia de ciberseguridad. Obtén más información: (enlace) #CybersecurityAwarenessMonth #SecureOurWorld
10. Vamos a #SecureOurWorld durante el #CybersecurityAwarenessMonth y proteger a los miembros mayores de la familia hablando sobre seguridad en línea. Diles a los miembros de tu familia que está bien preguntar si un correo electrónico, un mensaje de texto o una llamada son reales. Ninguna organización legítima solicita información personal mediante un mensaje de texto o una llamada telefónica. #phishing

Autenticación multifactor

11. Una de las cosas más fáciles que harás hoy es activar la autenticación multifactor (MFA, por sus siglas en inglés). Obtén más información: (enlace) #CybersecurityAwarenessMonth #SecureOurWorld
12. Tu contraseña puede ser segura, pero tu contraseña + la autenticación multifactor lo es aún más. Obtén más información aquí: (enlace) #CybersecurityAwarenessMonth #SecureOurWorld
13. Cuando habilitas la MFA, deshabilitas a los hackers. Incluso las soluciones rápidas, como la autenticación multifactor, son una defensa fuerte. #CybersecurityAwarenessMonth #SecureOurWorld

Contraseñas/Administradores de contraseñas

14. Usar la misma contraseña para todo puede ser fácil de recordar, pero también es fácil de hackear. Almacenar varias contraseñas en un solo administrador de contraseñas es más seguro y más fuerte. Obtén más información: (enlace) #CybersecurityAwarenessMonth #SecureOurWorld
15. Haz que la única contraseña que tengas que recordar sea la contraseña para acceder a tu caja fuerte. Almacena cientos de contraseñas diferentes en un administrador de contraseñas y haz que sea más fácil para ti. Obtén más información: (enlace) #CybersecurityAwarenessMonth #SecureOurWorld
16. Hacer 50 copias de la llave de tu casa probablemente sea excesivo. Usar la misma contraseña 50 veces también es una mala idea. Utiliza contraseñas que sean seguras, largas, únicas y aleatorias para cada sitio o cuenta. Esta es la mejor manera de mantener tus cuentas seguras. Obtén más información: (enlace) #CybersecurityAwarenessMonth #SecureOurWorld

Actualizaciones de software

17. Deja que las actualizaciones de software hagan el trabajo pesado por ti. ¡Es así de fácil! Al mantener tu tecnología actualizada, ¡obtendrás la mejor seguridad disponible! Obtén más información: (enlace) [#CybersecurityAwarenessMonth](#) [#SecureOurWorld](#)
18. Cuando activas las actualizaciones automáticas directamente desde tu dispositivo, no tendrás que preocuparte por obtener la última y mejor seguridad. Obtén más información: (enlace) [#CybersecurityAwarenessMonth](#) [#SecureOurWorld](#)
19. ¡Fuera lo viejo, dentro lo nuevo! Mantener tu software actualizado garantiza que obtendrás la mejor seguridad disponible. Obtén más información: (enlace) [#CybersecurityAwarenessMonth](#) [#SecureOurWorld](#)

Phishing

20. Hay algo muy satisfactorio en bloquear, eliminar y denunciar un ataque de phishing. Cuando veas uno, ¡pruébalo! Obtén más información: (enlace) [#CybersecurityAwarenessMonth](#) [#SecureOurWorld](#)
21. Algunos tipos de phishing son fáciles de detectar, mientras que otros tienen un gran camuflaje. Mantente alerta reconociendo las señales. Obtén más información: (enlace) [#CybersecurityAwarenessMonth](#) [#SecureOurWorld](#)
22. Los hackers utilizan cebos convincentes para intentar atraparte. ¡No te dejes engañar! Aprende a reconocer un caso de phishing y qué hacer con él: (enlace) [#CybersecurityAwarenessMonth](#) [#SecureOurWorld](#)