#JuntosPorTuSeguridadDigital | Contraseñas seguras | Enlaces sospechosos | Descargar apps de fuentes no oficiales | Ceder datos personales en Internet | Contactos desconocidos en Redes Sociales | **Doble factor de autentificación** | Actualiza tus dispositivos| Criptoactivos | Fake News

¿Sabes cómo puede protegernos el doble factor de autentificación (2FA)?

¡Te lo explicamos!

Consecuencias

Riesgo de violación de la cuenta:

Sin el 2FA, las cuentas son más susceptibles a ser comprometidas por ciberdelincuentes que puedan obtener acceso a las credenciales de inicio de sesión.

Mayor riesgo de robo de identidad:
Los ciberdelincuentes pueden usar tus credenciales robadas para hacerse pasar por ti, lo que podría resultar un robo de identidad, fraude o acceso no autorizado a tus datos personales y financieros.

Daño a la reputación:
Si tu cuenta está comprometida y se utilizan para realizar actividades maliciosas, esto podría dañar tu reputación personal o profesional, especialmente si la cuenta comprometida está asociada con tu identidad online o tu trabajo.

Pérdida de acceso a servicios:
En algunos casos, si una cuenta está comprometida, el proveedor de servicios podría bloquear el acceso a esa cuenta para protegerla, lo que podría resultar en la pérdida de acceso a servicios importantes o datos almacenados en esa cuenta.

Consejos

Activa tu DOBLE FACTOR de autentificación

El doble factor de autenticación (en inglés Two Factor Authentication o 2FA), también llamado autenticación de dos pasos, es una medida de seguridad que sirve para verificar la identidad de la persona que quiere ingresar a una cuenta.

Añade una segunda capa de protección

- El doble factor de autenticación añade una segunda capa de protección, reforzando el nivel de seguridad de nuestras cuentas de usuario y de nuestros datos personales.
- Esto lo logra utilizando dos métodos distintos para validar nuestra identidad.
- El primer método generalmente es una contraseña segura, y el segundo podría ser un código obtenido a través de un correo electrónico, un mensaje de texto o reconocimiento facial, entre otros.
- En resumen, no tener activado el 2FA aumenta significativamente el riesgo de compromiso de la cuenta y puede tener consecuencias graves en términos de ciberseguridad.
- El 2FA es una medida importante para agregar una capa adicional de protección a tus cuentas online.

Recursos

- Infografía ciberconsejos sobre doble factor de autentificación (2FA)
- Tríptico ciberconsejos sobre doble factor de autentificación (2FA)

- Vídeo ciberconsejos sobre doble factor de autentificación (2FA)