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

Consecuencias

Infección por malware: Los enlaces maliciosos pueden llevar a sitios web que intentan instalar malware en tu dispositivo que puede robar información confidencial, dañar archivos o incluso tomar el control completo de tu dispositivo.

Robo de datos personales: Al pinchar en un enlace malicioso, puedes ser redirigido a un sitio web falso diseñado para robar tus credenciales de inicio de sesión, información bancaria u otros datos personales.

Compromiso de la cuenta: Si proporcionas tus credenciales de inicio de sesión en un sitio web falso, los ciberdelincuentes pueden acceder a tu cuenta y realizar acciones no autorizadas en tu nombre.

Extorsión o chantaje: Al pinchar en enlaces maliciosos, podrías ser redirigido a sitios web que intentan extorsionarte o chantajearte. Por ejemplo, podrías ser víctima de ransomware, donde los ciberdelincuentes cifran tus archivos y exigen un rescate para restaurar el acceso a ellos.

Daño a la reputación: Si caes en una estafa a través de un enlace malicioso, esto podría resultar un daño a tu reputación personal o profesional. Por ejemplo, podrías ser víctima de una estafa de phishing que lleva a la divulgación involuntaria de información confidencial, lo que podría afectar tu credibilidad y confianza en línea.

Consejos

Mantén actualizados tus dispositivos: Configura tus dispositivos para que descarguen e instalen automáticamente las actualizaciones del sistema operativo y del software cuando estén disponibles. Esto garantiza que estés siempre protegido con las últimas correcciones deseguridad y mejoras.

Limita la información personal que compartes en internet: Muchas veces no somos conscientes de la cantidad de información personal que compartimos en internet, especialmente en redes sociales. Toda esa información puede usarse, según el actor que la recopile, con diferentes objetivos; desde crear perfiles de usuario para bombardearnos con publicidad personalizada, hasta crear campañas de phishing más dirigidas y personalizadas, o llevar a cabo fraudes de suplantación de identidad.

Recursos

- Infografía conexiones seguras
- Tríptico conexiones seguras
- Vídeo sobre conexiones seguras