Consecuencias

¡Protégete ante phishing!

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

¡No caigas en la trampa! Piénsalo bien antes de pinchar.

Antes de hacer clic:

Verifica el remitente:

En cualquier enlace en un correo electrónico, mensaje o publicación en redes sociales, verifica la autenticidad del remitente. Presta atención a la dirección de correo electrónico o nombre de usuario para detectar posibles discrepancias o signos de falsificación.

Analiza la URL:

Antes de pinchar en un enlace, pasa el cursor sobre él (sin hacer clic) para ver la URL completa.

Desconfía de los mensajes urgentes:

Los mensajes que intentan generar un sentido de urgencia o miedo, como advertencias de seguridad falsas o solicitudes de información personal inmediata, son comunes en los ataques de phishing.

Utiliza herramientas de seguridad:

Instala y mantén actualizado un software antivirus o antimalware en tus dispositivos.

"Al seguir estas recomendaciones y mantener una actitud cautelosa al interactuar con enlaces online, puedes reducir significativamente el riesgo de caer víctima de ataques de phishing y otros ataques maliciosos"

Recursos

- Infografía enlaces sospechosos
- Tríptico enlaces sospechosos
- Vídeo enlaces sospechosos