
ABIERTOS
AL SECTOR
PÚBLICO Y
SUS FAMILIARES
TIPS DE
CIBERSEGURIDAD
CoopeJudicial
AHORA PODÉS

LOS RIESGOS DE CONECTARSE A UNA RED WI-FI PÚBLICA.

Las redes Wi-Fi (redes inalámbricas) públicas, como las que encuentras en cafeterías, aeropuertos y centros comerciales, **son convenientes, pero también peligrosas.** La mayoría de estas redes no están cifradas, lo que significa que cualquier persona con conocimientos básicos de hackeo puede interceptar la información que transmites. **Esto incluye contraseñas, correos electrónicos, y datos financieros,** lo que puede llevar a suplantación de identidad o pérdidas económicas.

Además, **los ciberdelincuentes pueden crear redes Wi-Fi falsas,** conocidas como **"Evil Twins" (Gemelos Malvados),** que parecen legítimas, pero están diseñadas para capturar tus datos. Al conectarte a estas redes, podrías estar compartiendo información sensible directamente con los hackers sin darte cuenta. **Es crucial ser cauteloso al elegir una red y confirmar siempre que la red es legítima.**

Para protegerte al utilizar Wi-Fi público, **evita acceder a cuentas sensibles como las bancarias o realizar compras en línea.** Si es absolutamente necesario, considera el uso de una VPN (Red Privada Virtual), que cifrará tu conexión, haciendo mucho más difícil que alguien pueda interceptar tus datos.

CoopeJudicial
AHORA PODÉS

EL CUIDADO DE LA CONTRASEÑA

Las contraseñas son la primera línea de defensa contra el acceso no autorizado a tus cuentas en línea. Utilizar contraseñas fuertes y únicas es esencial para proteger tu información. Una buena contraseña debe ser lo suficientemente compleja, combinando letras mayúsculas y minúsculas, números y símbolos. Evita usar palabras comunes o información personal fácil de adivinar, como tu nombre, fecha de nacimiento, o "123456".

10 CONSEJOS PARA ESCRIBIR CONTRASEÑAS CORRECTAS

1. **No utilizar solo números**
2. **No utilizar solo letras o palabras**
3. **Optar por convinaciones alfanumericas**
4. **Intercalar signos de teclado**
5. **Mejor usa claves aleatorias**
6. **No utilizar la misma contraseña**
7. **Guardar las claves en un documento**
8. **Cuidado con las sesiones abiertas**
9. **No poner nuestro nombre**
10. **No poner fechas especiales**

RECUERDA USAR SIEMPRE INTERNET DE FORMA SEGURA

Reutilizar contraseñas en múltiples cuentas es un error común que puede tener graves consecuencias. Si un ciberdelincuente logra obtener tu contraseña en un sitio web menos seguro, podría intentar utilizarla en otras plataformas, accediendo así a más de tus cuentas. Para evitar esto, utiliza contraseñas únicas para cada cuenta y considera el uso de un gestor de contraseñas para mantenerlas seguras y organizadas.

Finalmente, habilita la autenticación de dos factores (2FA) siempre que sea posible. Esta medida añade una capa extra de seguridad al requerir un segundo paso de verificación, como un código enviado a tu teléfono, además de la contraseña. Cambia tus contraseñas regularmente y mantén tu información personal segura.

CoopeJudicial
AHORA PODÉS

INGENIERÍA SOCIAL Y SUPLANTACIÓN DE IDENTIDAD

La ingeniería social es una técnica que los ciberdelincuentes utilizan para manipular a las personas y obtener información confidencial. A través de correos electrónicos, llamadas telefónicas o mensajes falsos, se hacen pasar por entidades confiables, como bancos o empresas conocidas, para engañarte y robarte información personal. Este tipo de ataques **son peligrosos porque se basan en la confianza y el descuido humano,** no en fallos técnicos.

La suplantación de identidad es una de las consecuencias más graves de la ingeniería social. Los atacantes pueden usar **la información que obtienen para abrir cuentas bancarias, solicitar préstamos o realizar compras a tu nombre,** causando graves problemas financieros y legales. Recuperar tu identidad después de un robo puede ser un proceso largo y complicado, lo que subraya la importancia de **ser cauteloso con la información que compartes.**

PARA PROTEGERTE

Siempre verifica la autenticidad de las solicitudes de información, especialmente si llegan de manera inesperada.

No compartas detalles personales por teléfono, correo electrónico o mensajes de texto si no estás absolutamente seguro de la identidad del solicitante.

Mantén un escepticismo saludable y recuerda que las instituciones legítimas nunca te pedirán información confidencial de manera improvisada o insegura.

CoopeJudicial
AHORA PODÉS


CoopeJudicial
AHORA PODÉS