[INFOGRAFÍA] Protección de datos en vacaciones: cómo mantener tu información segura

12/07/2024

Actualidad

Las vacaciones son una época para relajarse y desconectar de las preocupaciones diarias. Sin embargo, en un mundo digitalizado es importante no bajar la guardia en lo que respecta la protección de datos y la seguridad de la información. Por esa razón, la Oficina de Protección de Datos junto con el Responsable de Seguridad de la Información presentan en forma de infografía las indicaciones básicas de como evitar situaciones de riesgo para la protección de datos personales en vacaciones:

Cómo mantener tu información segura:

- **Sé cuidadoso con lo que compartes en redes sociales**
  – Recuerda que publicar fotos en redes sociales sin el consentimiento de la persona puede generar responsabilidad sobre la protección del honor, la intimidad y la propia imagen.
- **No des detalles sobre tu geolocalización a través de redes o aplicaciones.**
  – Configura la privacidad en tus redes sociales y aplicaciones para limitar quien puede ver tu información.
  – Evita dar detalles sobre tu ubicación, fechas de viaje o documentos con datos personales o códigos de barras que puedan revelar tu identidad (billetes, tarjetas de embarque, etc.).
- **Evita conectarte a Wi-Fi publicas**
  – Las redes Wi-Fi públicas, como las de aeropuertos, estaciones de autobuses o de trenes, hoteles, cafeterías, pueden ser terreno fértil para los ciberdelincuentes y, recuerda que, la información que transmites por estas redes (contraseñas, datos financieros, etc.) puede ser fácilmente interceptada.
  – Siempre que sea posible utiliza tu red de datos móvil o conéctate a través de

una VPN para cifrar tu conexión y hacerla más segura.

- **Protege tus dispositivos**
  – Desactiva la opción de conexión automática a redes Wi-Fi y Bluetooth en tus dispositivos para reducir el riesgo de ataques.
  – Bloquea el dispositivo y/o la pantalla siempre que no esté en uso, evita las estaciones de carga pública y no olvides cifrar los dispositivos de almacenamiento permanente extraíbles.
- **Cuidado con el phishing**
  – Desconfía de los correos electrónicos que soliciten tu información personal o financiera y no hagas clic en enlaces sospechosos.
- **Contraseñas seguras:**
  – Si necesitas almacenar alguna clave, hazlo de forma segura, por ejemplo, un móvil protegido con contraseña o huella.
  – Chequea con cierta regularidad tus cuentas para detectar accesos no autorizados o actividad sospechosa.

[Descargue la infografía en PDF]

Para mas información sobre estas cuestiones pueden ponerse en contacto tanto con la **Oficina de Protección de Datos** (@email) , como con el Delegado de Protección de Datos (@email) y con el Responsable de Seguridad de la Información de la Universidad de Granada (@email)