Publicado en Madrid el 12/07/2023

Kaspersky advierte del peligro de usar puertos de carga USB y Wi-Fi públicas en vacaciones

Las vacaciones de verano es uno de los momentos en los que más se utilizan los dispositivos electrónicos. Por ello, y ante los viajes a otros países y el cambio en las rutinas, es importante mantenerse alerta de cara a posibles riesgos relacionados con la ciberseguridad que pueden poner en peligro la privacidad de información sensible, como datos bancarios o fotos y conversaciones personales

Las vacaciones puede ser el momento perfecto para desconectar de los dispositivos electrónicos. Sin embargo, se trata de una de las épocas en las que más se utilizan, ya sea para hacer fotos de una puesta de sol y publicarlas en redes sociales, pagar en hoteles y restaurantes o escuchar música dando un paseo junto al mar. Sin embargo, los expertos de Kaspersky recuerdan que es importante mantener la cautela a la hora de utilizar redes Wi-Fi públicas o realizar determinadas transacciones para evitar que los ciberdelincuentes aprovechen los descuidos y se hagan con datos e información privada y sensible.

De hecho, entre las principales preocupaciones de los españoles en lo referente a sus smartphones, se encuentran el robo de sus datos bancarios (85,5%), perder todas las fotos y vídeos (54,5%) o que un ciberdelincuente pueda acceder a dicho material gráfico almacenado en sus dispositivos (40%), según el informe 'Influencia de la tecnología en la vida de los españoles', elaborado por Kaspersky entre más de 2000 españoles.

Por este motivo, los expertos de la compañía de ciberseguridad explican cómo eludir a los ciberdelincuentes que se aprovechen de los despistes de los usuarios durante las vacaciones de verano:

Evitar cargar el móvil en USB públicos. Muchas personas caen en la tentación de utilizar puertos USB públicos para cargar sus teléfonos móviles mientras están de viaje, por ejemplo, en aeropuertos, trenes o cafeterías. Sin embargo, estos puntos de carga pueden ser una fuente potencial de ataques cibernéticos. Muchos ciberdelincuentes instalan malware directamente en ellos para acceder a los dispositivos que se conectan y robar información confidencial de los usuarios. Por ello, una buena idea es meter en la maleta una batería portátil que ahorre riesgos innecesarios.

No hacer transacciones desde Wi-Fi públicas. Conectarse a este tipo de redes puede ser muy conveniente para revisar correos electrónicos, realizar transacciones bancarias o acceder a redes sociales durante las vacaciones, especialmente en países en los que no se dispone de roaming. No obstante, las Wi-Fi públicas son vulnerables y pueden ser fácilmente interceptadas por ciberdelincuentes. Además, hay que ser especialmente cauteloso a la hora de acceder a la banca online o hacer compras en Internet. Lo mismo ocurre si se realizan consultas relacionadas con el trabajo, ya que los ciberdelincuentes pueden acceder a la información de la empresa. De hecho, según el informe Kaspersky 2022 IT Security Economics elaborado tras entrevistar a 3.000 responsables IT de 26 países, el 22% de las brechas de seguridad en las pymes fueron causadas por empleados durante el pasado año. Por ello, es importante contar con una solución de seguridad de confianza

actualizada y evitar utilizar redes públicas cuando se va a introducir o consultar datos e información delicados.

Cuidado al sacar dinero de cajeros. Cuando un usuario necesita efectivo durante las vacaciones, es común recurrir a los cajeros automáticos. Sin embargo, estos dispositivos también pueden ser objeto de manipulación por parte de delincuentes. Antes de utilizar un cajero, es aconsejable asegurarse de que sea uno confiable y ubicado en una zona segura. Muchos ciberdelincuentes infectan estos cajeros con malware como HydraPoS, conocido por clonar tarjetas de crédito, o RawPoS, el malware capaz de extraer la totalidad de los datos de la banda magnética de la memoria volátil. Así, los expertos también recomiendan inspeccionar el cajero en busca de elementos sospechosos, como cámaras incorporadas, y no aceptar ayuda de extraños mientras se realiza la transacción.

No perder de vista la tarjeta al pagar con datáfono. El uso de las tarjetas de crédito se multiplica durante los meses de verano: hoteles, restaurantes, coches de alquiler, actividades de ocio... Momentos en los que es común que los delincuentes realicen prácticas como el skimming, que consiste en copiar la información de las tarjetas de crédito o débito mientras se realizan transacciones. Para evitar esto, no hay que perder nunca de vista la tarjeta al pagar con un datáfono y mucho menos que la lleven a otro lugar para realizar el cobro. Si es posible, hay que utilizar métodos de pago más seguros, como pagos móviles o tarjetas con tecnología de chip, cubrir la mano a la hora de marcar el código secreto y nunca apuntar o compartir con terceros el pin.

"Se trata de aspectos que hay que tener en cuenta todo el año, pero especialmente en verano, cuando se viaja a otros países y bajamos la guardia debido a la desconexión y relajación propias de las vacaciones. Por lo tanto, es fundamental estar atentos y seguir prácticas como estas, que son sencillas y ayudan a proteger los datos personales y disfrutar de un verano sin preocupaciones", concluye Marc Rivero, Senior Security Researcher de Kaspersky.

Datos de contacto:
Mónica Iglesias
690196537

Nota de prensa publicada en: Madrid

Categorías: Internacional Nacional Viaje Madrid Ciberseguridad Dispositivos móviles