El Boletín Mensual de Concientización en Seguridad para ti

Consejos de ciberseguridad para las vacaciones

Resumen

Como la temporada de fiestas se acerca, millones de personas estarán viajando. Si tú eres una de ellas, aquí hay algunos consejos que te ayudarán a mantenerte seguro.

- **Dispositivos móviles**: Lleva tan pocos dispositivos como puedas. Entre menos dispositivos tengas contigo mientras viajas, será más difícil que los pierdas o te los roben. De hecho, ¿sabías que es mucho más probable que pierdas un dispositivo a que te lo roben? Siempre que salgas de la habitación del hotel, restaurante, bajes de un taxi, tren o avión, checa rápidamente que tengas todos tus dispositivos. No olvides incluir a tus amigos o familiares para que ellos revisen si llevan todos sus dispositivos también, los niños pueden haber dejado alguno debajo del asiento o en la mesa de algún restaurante.

  Para los dispositivos que decidas llevar contigo, asegúrate de actualizarlos para que tengan la última versión del sistema operativo y de las aplicaciones. Mantén activado el bloqueo de pantalla. Si es posible, asegúrate de tener alguna forma de poder rastrear los dispositivos en caso de que se pierdan. Adicionalmente, podrías querer activar la opción del borrado remoto. De esta manera, si pierdes un dispositivo o te lo roban, podrás ver su ubicación y/o borrar todos los datos sensibles y las cuentas del mismo. Finalmente, haz una copia de seguridad de cualquier dispositivo que lleves contigo y así, si llegas a perder alguno, podrás recuperar tu información fácilmente.

- **Conexiones Wi-Fi:** Cuando viajes, es posible que tengas que conectarte a una red Wi-Fi pública. Ten en mente que algunas veces no sabrás quién configuró la red, quién la está monitoreando y cómo, y quién más está conectado a ella. En lugar de conectarte a una red Wi-Fi pública, siempre que te sea posible conéctate y utiliza la función de punto de acceso personal de tu teléfono. De esta manera siempre tendrás una conexión Wi-Fi de confianza. Si eso no es posible y tienes que conectarte a una red pública (como en un aeropuerto, hotel o café) utiliza una Red Privada Virtual (del inglés Virtual Private Network), comúnmente llamada VPN. Este es un programa que instalas en tu computadora portátil o celular para ayudar a proteger y anonimizar tu conexión Wi-Fi. Algunas soluciones de VPN incluyen configuraciones para habilitar automáticamente la VPN cuando te conectas a redes Wi-Fi no confiables.

- **Computadoras públicas**: Evita usar equipos públicos, tal como aquellos en hoteles y cafeterías, para ingresar a cualquiera de tus cuentas o a información sensible. No sabes quién utilizó el equipo antes que tú y es posible que la hayan infectado accidental o deliberadamente con malware, como con un registrador de pulsaciones de teclas (denominado en inglés keylogger). Limítate a los dispositivos que controlas y en los que confías.

- **Redes sociales**: Nos encanta mantener al tanto a los demás sobre nuestros viajes y aventuras en redes sociales, pero no siempre sabemos quiénes son todos los amigos o espectadores en línea. Evita compartir de más durante las vacaciones tanto como sea posible y considera esperar para compartir el viaje hasta que estés en casa. Adicionalmente, no publiques fotografías de pases de abordar, licencias de conducir o pasaportes, ya que esto puede llevar al robo de identidad.

- **Trabajo**: Si vas a trabajar en vacaciones (¡Esperamos que no!) asegúrate de verificar con anticipación cuáles son las políticas para viajes de trabajo, incluidos los dispositivos o información que puedes llevar y cómo conectarte de forma remota a los sistemas de trabajo de manera segura.

Las vacaciones deberían ser un momento para relajarse, explorar y divertirse. Estos sencillos pasos te ayudarán a garantizar que lo hagas de forma segura.

Editor invitado

Princess Young es analista senior en Southwest Airlines, lidera los esfuerzos de educación y capacitación en ciberseguridad para 60,000 empleados en todo el país. Princess disfruta trabajar con los empleados para que puedan sentirse empoderados para compartir la responsabilidad de la ciberseguridad, independientemente de su función o título.

Recursos

Asegurando tus dispositivos móviles: https://www.sans.org/newsletters/ouch/securing-mobile-devices/
El Poder de actualizar: https://www.sans.org/security-awareness-training/resources/power-updating
Redes privadas virtuales (VPN): https://www.sans.org/newsletters/ouch/Virtual-Private-Networks/
¿Hacer respaldos?: https://www.sans.org/newsletters/ouch/got-backups/

Traducido para la comunidad por: Célica Martínez Aponte and Iván Galindo, UNAM-CERT