Ciberseguridad:

Seguridad en los desplazamientos

Este documento contiene información clave que necesitará para poder responder el cuestionario al final de esta viñeta. También puede descargar este documento.

Dispositivos móviles

¡El negocio es móvil! Los computadores portátiles, las tabletas y los teléfonos inteligentes permiten a las personas trabajar prácticamente desde cualquier lugar si su función lo permite. Aunque es ventajoso desde el punto de vista empresarial, esta movilidad conlleva un mayor riesgo y la necesidad de que los usuarios sean conscientes de su alrededor, del trabajo que realizan y del papel fundamental que desempeñan en la protección de Scotiabank y sus clientes.

VPN

Cuando trabaje a distancia utilizando un computador portátil propiedad del banco y administrado por éste, deberá conectarse siempre a la Red Privada Virtual (VPN) de Scotiabank. La VPN encripta y protege toda la comunicación entre su computadora portátil y la red interna de Scotiabank.

Wi-Fi

El Wi-Fi se ha vuelto omnipresente. Cafeterías, restaurantes, hoteles, comercios minoristas e incluso talleres mecánicos ofrecen Wi-Fi gratuito para el uso de sus clientes. Sin embargo, estas redes abiertas son intrínsecamente poco fiables porque no está claro quién más puede estar al acecho en esa red e intentar hackear a otros usuarios. Cuando trabaje a distancia, asegúrese de seguir estas normas a la hora de decidir a qué red Wi-Fi se va a conectar.

Conéctese a una red Wi-Fi conocida y de confianza, como la de su casa.

Cuando no esté en casa, favorezca las conexiones Wi-Fi de empresas de confianza (compruebe dos veces el nombre de la Wi-Fi, ya que los hackers a veces configuran redes inalámbricas con nombres similares para que se conecte directamente a ellas).

Tan pronto como se haya conectado a cualquier Wi-Fi, incluso la propia en casa, conéctese INMEDIATAMENTE a la red VPN de Scotiabank para asegurar todas las comunicaciones.

Viajar con dispositivos del Banco

Cuando viaje con sus dispositivos móviles, llévelos siempre consigo. No los deje sin supervisión y no los guarde en un vehículo. Los delincuentes disponen de dispositivos que pueden detectar los aparatos electrónicos en el interior de los vehículos, aunque estén apagados. Si se aloja en un hotel, utilice la caja fuerte de la habitación para asegurar sus dispositivos cuando no los esté utilizando.

Sitios web externos y medios sociales

No publique información interna o confidencial en ningún sitio web público o ajeno a Scotiabank, incluyendo las redes sociales.

Cualquier publicación en las redes sociales en la que usted se identifique como empleado de Scotiabank puede ser interpretada como si hablara en nombre del Banco y puede ser mal interpretada como si fuera la opinión del Banco. Consulte nuestro Código de Conducta de Scotiabank (nuestro “Código”) y las normas relativas a las conversaciones con los medios de comunicación y el público.