POPULAR BANK

# Guía de seguridad de la información
# Pistas de Seguridad

## *REGLAS DE PRECAUCION*

**CLAVES PRIVADAS O TOKEN**

- Su nombre de usuario, clave secreta o contraseña, número de identificación personal (PIN), Token son sus datos personales, privados e intransferibles. Protéjalos porque son valiosos.
- Son llaves de identificación y acceso a los sistemas del Popular Bank Ltd. Inc. (son usted mismo) y constituyen, por tanto, información confidencial que usted no debe compartir ni, mucho menos, facilitar a nadie a través de ningún mensaje de correo electrónico, SMS, red social, llamada telefónica o página en internet, pues esta información puede ser usada, sin su consentimiento, para realizar operaciones bancarias no autorizadas.
- Proteja las respuestas a las preguntas de seguridad que haya establecido, como medida alternativa de autenticación.
- Popular Bank Ltd. Inc. nunca le contactará por teléfono ni vía correo electrónico o SMS pidiéndole que divulgue todos o algunos de sus datos financieros o para acceso a las aplicaciones.
- Cerciórese de que no es observado mientras introduce sus datos financieros en nuestra, página en internet. Sepa que hay personas que se dedican a mirar a sus espaldas ("*shoulder surfing*") con la intención de captar sus datos privados o confidenciales.
- Al definir su contraseña o su PIN, no escoja opciones fáciles de deducir (sus nombres, apellidos, cédula, fecha de nacimiento o dígitos similares a su número telefónico). Preferiblemente combine las letras o palabras elegidas (alternando mayúsculas y minúsculas) con números y caracteres especiales.
- Cambie periódicamente su contraseña, al menos cuatro veces al año.
- No repita la misma contraseña para los distintos sistemas con los cuales usted interactúa.
- No anote su contraseña o PIN en ningún documento, dispositivo o sistema a los cuales otras personas pudieran tener acceso; ni siquiera al dorso de la tarjeta de débito.
- Rompa o triture cualquier nota o documento que usted vaya a desechar y que contenga, alguna o toda, su información financiera personal. Sepa que hay personas que se dedican a buscar entre la basura ("*dumpster diving*") en busca de datos o imágenes, queriendo actuar en nombre de usted, usurpando su identidad, para realizar transacciones por medio de sus cuentas bancarias.
- Introduzca sus datos financieros en entornos seguros.
- Guarde su Token en un lugar seguro.

**EQUIPOS**

- Mantenga actualizado el sistema operativo de su computadora e instale los parchos de seguridad periódicamente.
- Disponga de un antivirus en el equipo y actualícelo periódicamente según el período de actualización establecido por la marca usada por usted.
- Utilice una pared de fuego (*firewall*) para protegerse de posibles ataques mientras navega en la Internet.
- Cuando termine de usar su computadora, apáguela completamente y no la deje en modo de hibernación. Recuerde que AHORRAR Nos hace bien ("El ahorro de energía contribuye a disminuir los gases de efecto invernadero").
- Realice transacciones bancarias sólo en computadoras confiables. Las computadoras públicas (en cafés, universidades, centros de internet, bibliotecas, etc.) deben ser usadas con precaución, debido a que son equipos de uso compartido y los archivos que se descarguen pudieran ser utilizados por cualquier persona y extraídos del equipo sin su autorización.
- Instale un programa Anti-Espía para evitar que se ejecuten archivos tipo espía (*spyware*) en su computadora.
- Tenga cuidado al abrir archivos con 2 o 3 extensiones en el nombre (por ejemplo: worldofwarcraft.jpg.exe) porque es muy probable que sea el disfraz que enmascare un software malicioso.
- Periódicamente, resguarde su información haciendo copias de seguridad en dispositivos externos (disco duro externo, CD, DVD, o memorias USB).
- No resguarde la copia de seguridad en la misma computadora, ya que en caso de un accidente podría perder toda la información almacenada.

**NAVEGACIÓN**

- Navegue en páginas en internet conocidas. Sea prudente al visitarlas, sobre todo si le solicitan que descargue programas u otro tipo de archivos para su funcionamiento.
- Cuando navegue en la internet, infórmese sobre la política de privacidad de cada página que visita; si es que decide interactuar a través de una, esta le debería explicar qué tipo de información suya recolecta, cómo se utiliza y si se comparte con terceras partes.
- No deje desatendida la computadora mientras está conectado a una página en internet que requiera de su usuario y contraseña para el acceso. Una vez termine de realizar sus transacciones, cierre la sesión y luego cierre por completo el navegador.
- Si va a alejarse de su computadora durante un buen rato, y no desea apagarla, bloquee la pantalla.
- No acepte la ejecución de programas cuya descarga se activa sin que usted lo solicite.
- Conozca sobre la existencia de virus engañosos ("*hoaxes*").
- No facilite sus datos personales en páginas en red cuya dirección electrónica (URL) no incluya la "s" (https://) y verifique que el certificado de seguridad corresponda a la página que está visitando.
- Cuando navegue desde una computadora pública recuerde borrar el historial de navegación. Si lo hace en su computadora personal, igualmente, elimine periódicamente los archivos temporales y *("cookies"*) que se instalan en cada sesión de navegación.

- Busque y desactive la función de Ajustes para el Control de la Privacidad o, bien, Almacenamiento Automático de Contraseñas. Lo normal es que deba quitar el cotejo al lado de la opción que cada navegador establece:

  - INTERNET EXPLORER
    Herramientas>Opciones de Internet>Contenido>Información personal>Autocompletar>Desactivar nombres de usuarios y contraseñas

  - MOZILLA FIREFOX
    Tools>Options>Security>Remember passwords for sites

  - GOOGLE CHROME
    Tools>Personal stuff>never save passwords.

- Actualice el navegador de su computadora, ya que además de mantener el nivel de cifrado recomendable para conexiones seguras, esta acción corregirá diferentes vulnerabilidades que hayan sido detectadas y resueltas por el proveedor de este.
- Actualice su programa de gestión de correo electrónico.
- Nunca acceda a la página de Popular Bank Ltd. Inc., desde enlaces contenidos en un correo electrónico.
- Al realizar transacciones bancarias o compras virtuales, compruebe que se encuentra en un entorno seguro, verificando que la página en internet que visita contiene los elementos propios de una sesión de comunicación cifrada.
  - El protocolo con que inicia la dirección electrónica contiene una “s” indicativa de seguro (https://) y
  - En la esquina inferior del navegador aparece el ícono de un candado cerrado o una llave.

**GENERAL**

- Popular Bank Ltd. Inc., nunca le solicitará que revele sus datos financieros personales a través de un correo electrónico.
- Siempre preste atención a los detalles de este tipo de mensajes. Tenga presente que hay páginas en internet diseñadas para engañarlo, pidiéndole que suministre sus datos personales y financieros.
- La naturaleza fraudulenta de los mensajes se refleja en la redacción de su contenido, en la composición de su dirección electrónica, que no es la oficial de Popular Bank Ltd. Inc., y en que el entorno de la página a la cual enlaza no posee los elementos propios de un sitio seguro.
- No abra correos electrónicos o archivos, ni pulse sobre enlaces, que provengan de remitentes desconocidos, inesperados o cuyo título carezca de sentido.
- Si recibe mensajes de correos electrónicos pidiéndole sus datos financieros, no facilite lo que le piden. Reporte inmediatamente lo ocurrido reenviando ese mensaje al correo electrónico phishing@bpd.com.do, y bórrelo de su computadora inmediatamente después.
- No se fíe de regalos o promociones fáciles de obtener, ni responda mensajes que soliciten con urgencia sus datos financieros personales.

- Nunca deje su cuenta de correo electrónico expuesta a los demás. Algún malintencionado podría sustraerle sus contactos, enviar mensajes inapropiados a nombre suyo o, incluso, interceptar algún correo electrónico en el cual aparezcan algunos o todos sus datos financieros personales.
- Revise periódicamente su programa gestor de correo electrónico, específicamente las Bandejas de Salida y de Correos Enviados, para detectar mensajes que usted no haya enviado. Si descubre alguna correspondencia desconocida, es un signo de que su computador pudiera estar infectado con un programa malicioso o que sus credenciales fueron sustraídas, por lo que debe a cambiar su contraseña de inmediato. Adicionalmente, actualice su programa antivirus y antispyware y realice una revisión de su equipo con estos softwares.
- Reporte inmediatamente la pérdida de sus chequeras o cheques Tome las precauciones necesarias para detectar y eliminar la invasión, desconectándose de la internet y corriendo los programas antivirus y anti-espía.