Documento de Consejos de Seguridad para canales electrónicos.

En Internet:

• No divulgues tus claves, las mismas son personales e Intransferibles.
• No dejes tus claves anotadas en papeles o agendas ni en tu tarjeta. No la dejes registrada en tu PC, ya que cualquier virus (Programa Malicioso) podría sin que lo notes tomar esta información y re transmitirla a un atacante.
• Es conveniente que cambies tu clave periódicamente, esto incrementará tu seguridad en el Canal.
• Si considerás que alguien vio o conoce tu clave cambiala inmediatamente.
• No respondas ningún tipo de E-mail donde te sean requeridos datos de tarjetas, o claves aunque te adviertan de un posible problema, argumentando la necesidad de actualizar tu información.
• Tratá de no utilizar números que sean fáciles de averiguar como: correlativos, series repetidas de un mismo número, fechas de nacimiento, aniversarios, direcciones, patentes de vehículos o algún otro dato que pueda ser vinculado de forma unívoca a vos.

En el Teléfono:

• No informes tus claves ni datos personales o bancarios a nadie, si vos no iniciaste la llamada o puedas asegurar el origen de la misma.
• Si recibís una llamada sospechosa a nombre de Wilobank, no la respondas inmediatamente al número de teléfono recibido, tomate tu tiempo para verificar los números correctos del Banco y recién ahí comunicate a los números de teléfono que dispusimos para vos.
• Si necesitás comunicarte con nosotros, no utilices el celular de otra persona, los números que digites en la pantalla del mismo pueden quedar registrados y de esta forma ser comprometidos por terceros.
• Siempre que necesites conversar con nosotros, hacelo llamando a los números que Wilobank publica en su portal, no utilices números de teléfono de lugares que no puedas corroborar su veracidad.

En el Celular

• No informes tus claves ni datos personales o bancarios a nadie, si vos no iniciaste la llamada o puedas asegurar el origen de la misma.
• No guardes el usuario o la clave del servicio en tu celular.
• Tratá de no almacenar información financiera en tu celular
• Si recibís una llamada sospechosa a nombre de Wilobank, no la respondas inmediatamente al número de teléfono recibido, tomate tu tiempo para verificar los números correctos del Banco y recién ahí comunícate a los números de teléfono que dispusimos para vos.
• Si necesitás comunicarte con nosotros, no utilices el celular de otra persona, los números que digites en la pantalla del mismo pueden quedar registrados y de esta forma ser comprometidos por terceros.
• Siempre que necesites conversar con nosotros, hacelo llamando a los números que Wilobank publica en su portal, no utilices números de teléfono de lugares que no puedas corroborar su veracidad.
• En el teléfono No informes tus claves ni datos personales o bancarios a nadie, si vos no iniciaste la llamada o puedas asegurar el origen de la misma.
• Si recibís una llamada sospechosa a nombre de Wilobank, no la respondas inmediatamente al número de teléfono

recibido, tomate tu tiempo para verificar los números correctos del Banco y recién ahí comunícate a los números de teléfono que dispusimos para vos.
• Si necesitás comunicarte con nosotros no utilices el celular de otra persona, los números que digites en la pantalla del mismo pueden quedar registrados y de esta forma ser comprometidos por terceros.
• Siempre que necesites conversar con nosotros, hacelo llamando a los números que Wilobank publica en su portal, no utilices números de teléfono de lugares que no puedas corroborar su veracidad.
• En caso de que extravíes tu celular, comunicate de inmediato con tu operador y solicitá el bloqueo del mismo de manera urgente.

En Cajeros Electrónicos.

• Fuera del horario bancario, te sugerimos utilizar cajeros en lugares con gran movimiento (Shoppings, Estaciones de Servicio).
• No introduzcas tu tarjeta si el cajero está fuera de servicio.
• Durante la operación mantenete cerca de la pantalla a fin de evitar que otras personas vean lo que digitás.
• No olvides al finalizar la operación, retirar la tarjeta y guardarla inmediatamente.
• No aceptes ayuda de extraños.
• No dejes o tires los tickets de tu transacción en el lobby del cajero.
• Antes de retirarte del Cajero verificá que tengas la tarjeta en tu poder.
• En caso de que tu tarjeta haya sido retenida por el cajero debés realizar la denuncia a red LINK, comunicándote a 0810-666-9262.

Protege tu PC´s, Notebook, Celular o Tablet

• Instala un antivirus, programas de bloqueo de acceso desde Internet (Firewall) y protege el acceso utilizando contraseñas
• Utiliza siempre software originales y actualizados cada vez que existan nuevas versiones
• No instales aplicación que desconozcas su origen, que no provengan de tiendas oficiales.
• Mantene tus dispositivos siempre al alcance de tu vista, evita su perdida y el acceso de terceros
• SI los vas a descartar, Tirar o donar, tener en cuenta eliminar previamente la información de los mismos, para tal fin existen diferentes tipos de software que realizan esta tarea.

Como saber si mi dispositivo está infectado:

• Si tiene un comportamiento inusual, mayor lentitud, muestra mensajes repentinos, envía mensajes de correo electrónico sin tu conocimiento
• Si aparecen iconos sin que hubieras instalado nada previamente

Como me deshago del Malware o Virus

Mantene siempre actualizado tu sistema Operativo y tu antivirus, ejecútalo de forma periódica, Elimina todo lo que el Anti Virus identifique como problema.