



## **BANESCO COMPARTE RECOMENDACIONES PARA EVITAR EL FRAUDE CIBERNÉTICO**

**En momentos de vulnerabilidad, los fraudes cibernéticos aumentan. Banesco recuerda a sus clientes las medidas que recomienda para cuidar sus productos financieros y priorizar la ciberseguridad.**

Banesco Banco Universal, institución bancaria de capital 100 % venezolano, recuerda la importancia de cuidar la información financiera de cada cliente y el uso de sus productos, en momentos de vulnerabilidad. En situaciones como la que vive el país y sus ciudadanos - luego de los terremotos del 24 de junio - donde se crean múltiples canales de solicitud de aporte económicos, es común el auge de los fraudes cibernéticos. Por ello, la institución financiera recuerda los siguientes consejos de ciberseguridad para proteger la información y las operaciones de sus clientes.

### **Cuídese de la usurpación de identidad o *phishing***

El *phishing* es un método de estafa aplicado por usurpadores que se hacen pasar por una institución de confianza a través de un correo electrónico, mensajería de texto o llamada telefónica, para acceder a datos financieros. Una acción común es el envío masivo de correos promocionales o mensajes de WhatsApp con premios o descuentos engañosos para que el usuario suministre sus datos personales. También aplica el envío de códigos con la excusa de la verificación de cuentas de WhatsApp.

Ante la duda de una estafa de esta naturaleza es importante verificar la cuenta de correo que envía el mensaje. Si se trata de una institución o empresa, su dirección de correo debe coincidir con el URL de la institución. En caso de que desconozca la fuente o persona que envía el correo, no responda a él y obvie los enlaces enviados por esta vía. No utilice buscadores para ubicar la plataforma de Banesco, prefiera escribir la dirección de la página directamente.

### **Mantenga en privado sus datos personales**

Evite responder a correos electrónicos, llamadas telefónicas o mensajes de texto que solicitan información confidencial como: claves, contraseñas, números de tarjetas de crédito o débito, códigos de acceso o ingresar a sitios no oficiales del banco.

Se recomienda cambiar regularmente la contraseña de la banca en línea y de los correos asociados a las cuentas financieras. En el caso de Banesco, la banca digital le avisará cuando sea necesario renovar su clave a través de la misma plataforma. Evite anotar la nueva contraseña o acceder a la banca en línea desde lugares públicos. Instalar o actualizar el antivirus es otra medida que favorece a la seguridad.

### **Priorice el uso de la banca digital y BanescoMóvil**

El uso de computadoras en espacios públicos o compartidos como cibercafés, representan un riesgo para los datos del cliente. Para consultar saldo, realizar operaciones o confirmar transacciones, es mejor hacer uso de la aplicación de BanescoMóvil. En aquellos casos

donde el usuario utilice un equipo compartido, se sugiere cerrar todas las ventanas del navegador y realizar limpieza de *cookies*, historial y archivos, al finalizar la conexión.

### **Confíe en cuentas verificadas para sus donaciones**

En caso de que desee contribuir con aportes para los afectados por los terremotos, utilice canales verificados para eso. Banesco pone a su disposición canales de apoyo a través del Dividendo Voluntario para la Comunidad y la Cruz Roja Venezolana.

Para contribución a la campaña Fuerza Venezuela, que lidera el Dividendo Voluntario para la Comunidad en alianza con Cáritas Venezuela, Banesco pone a disposición la cuenta del DVC para aportes directos:

Dividendo Voluntario para la Comunidad, A.C.

J-070133805

0134-0031-860311165203

Por su parte, a través de la campaña “Duplica tu impacto”, la entidad financiera se une a la acción de la Cruz Roja Venezolana, duplicando el aporte de cada persona que contribuya con las acciones de esta organización mundial:

Banesco Banco Universal

J-070133805

0134-0008-37-0081096451

Como medida de seguridad adicional, es importante la activación del Doble Factor de Autenticación de las cuentas bancarias y mantener actualizados los datos personales, el sistema operativo y navegador del móvil o computadora. Revisar periódicamente los movimientos de cuentas y tarjetas es una buena práctica ante el fraude cibernético.

Evite responder a correos electrónicos, llamadas telefónicas o mensajes de texto que solicitan información confidencial como: claves, contraseñas, números de tarjetas de crédito o débito, códigos de acceso o ingresar a sitios no oficiales del banco. Ante cualquier sospecha de fraude, puede escribir a [monitoreodefraude@banesco.com](mailto:monitoreodefraude@banesco.com) o comunicarse por el (0212) 501.10.29.

Para más información sobre medidas de seguridad bancaria, visite [Banesco.com](http://Banesco.com).

Encuétranos como



BanescoBancoUniversal



Banesco Banco Universal



@Banesco



Banesco Banco Universal



Banescoenimágenes