CAVECOM-E | COMUNICADO OFICIAL
Caracas, mayo de 2025

ALERTA DE CIBERSEGURIDAD BANCARIA

Nuevas formas de estafa digital están en aumento en Venezuela: aprende a protegerte.

Desde la Cámara Venezolana de Comercio Electrónico (Cavecom-e) queremos alertar a los ciudadanos, empresas, instituciones bancarias y comercios sobre el aumento de estafas digitales avanzadas que están afectando a miles de personas en todo el país. Estas amenazas no solo atacan computadoras o redes, sino que también están dirigidas directamente a ti como usuario o trabajador.

¿QUÉ ESTÁ PASANDO?

En los últimos días se han detectado múltiples casos de Amenazas Persistentes Avanzadas (APT), pero también de fraudes directos al usuario, donde los ciberdelincuentes usan ingeniería social para engañarte y robar tu información bancaria. Estas son algunas de las modalidades más comunes:

1. VISHING (FRAUDE POR LLAMADA TELEFÓNICA):

Te llaman diciendo que son del banco, te dicen que tu cuenta ha sido bloqueada o detectaron movimientos sospechosos. Te piden que confirmes tu número de tarjeta, clave o código de seguridad, y así roban tu cuenta.

2. SMISHING (FRAUDE POR MENSAJE DE TEXTO):

Recibes un SMS con un enlace que dice: “Tu cuenta ha sido suspendida. Ingresa aquí para activarla: bancoseguro-venezuela.link”.Al entrar, te lleva a una página falsa muy parecida al portal del banco.

3. SPEAR PHISHING (CORREO PERSONALIZADO):

Te llega un correo con tu nombre y datos reales, simulando ser del banco o una empresa que conoces, y te invitan a descargar un archivo o actualizar tus datos.

4. SIMULACIÓN DE BLOQUEO BANCARIO:

Te hacen creer que tu cuenta fue bloqueada, y luego te llaman “amablemente” para ayudarte. Así logran que entregues tu información personal o bancaria sin darte cuenta.

5. CAMPAÑAS FALSAS PAGADAS EN REDES SOCIALES:

Últimamente están circulando publicaciones pagadas (anuncios) en Instagram, Facebook o TikTok que simulan ser de bancos reconocidos y ofrecen supuestas promociones, créditos rápidos o regalos por llenar formularios.

¡CUIDADO! ESTAS CAMPAÑAS:

- Usan logotipos y colores reales de los bancos.
- Te llevan a páginas falsas para robar tus datos o infectar tu teléfono.
- Son lanzadas desde cuentas falsas sin seguidores ni verificación oficial.

¿CÓMO DETECTARLAS?

- Revisa si la cuenta tiene el check azul de verificación.
- Verifica que tenga seguidores reales y publicaciones antiguas.
- Nunca entregues tus datos personales o bancarios por promociones en redes.
- Si dudas, llama tú directamente al banco.

6. COMPROBANTES DE PAGO FALSOS:

Se ha detectado un aumento en el uso de comprobantes de pago falsos, especialmente en transacciones con empresas y comercios. Los delincuentes simulan transferencias con capturas de pantalla alteradas o montajes digitales muy convincentes, haciendo creer que el pago ha sido realizado.

¡ATENCIÓN EMPRESAS Y COMERCIOS!

* No confíes únicamente en una imagen de comprobante.
* Verifica siempre en la banca en línea o espera la notificación oficial de tu banco.
* Establece protocolos internos para validar cada operación antes de liberar productos o servicios

7. ALERTA A LOS GRUPOS DE WHATSAPP

Se ha detectado un aumento de estafas en los grupos de Whatsapp ya que estos grupos exponen tu contacto y tu número telefónico, y los ciberdelincuentes se cuelan en grupos sociales, vecinales, cursos, eventos pagos inclusive, donde llegan a pagan su inscripción y valiéndose de ese status te indican que has sido calificado para un nivel superior y que solo necesitan el código que les va a llegar para validar su nuevo status y hachear tu wahatsapp, este es uno de los ejemplos más recurrentes, por lo que alertamos a no dar ningún CODIGI por Whatsapp así estés en un grupo de conocidos.

¿QUÉ PUEDES HACER PARA PROTEGERTE?

Desde Cavecom-e te damos estos consejos simples pero poderosos:

- Nunca compartas tus claves ni códigos de seguridad por teléfono, whatsapp, mensaje ni correo, aunque parezcan oficiales.
- No abras enlaces ni descargues archivos de correos o mensajes sospechosos.
- No atiendas llamadas inesperadas del banco. Cuelga y llama tú al número oficial.
- Activa el doble factor de autenticación (2FA) en todos tus servicios.
- Desconfía de ofertas bancarias que aparecen como publicidad pagada y verifica siempre en los canales oficiales.
- Cambia tus claves frecuentemente y no uses la misma para todo.
- Comparte esta información con tus familiares y compañeros de trabajo.

¿Y LOS BANCOS QUÉ DEBEN HACER?

A todas las entidades financieras y proveedores tecnológicos, Cavecom-e recomienda:

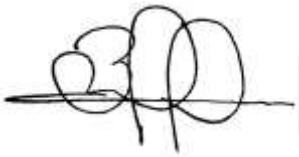
- Fortalecer sus equipos de monitoreo antifraude en redes sociales.
- Reportar de inmediato cualquier cuenta falsa suplantando su identidad.
- Aumentar campañas educativas a clientes.
- Ejecutar simulacros internos de spear phishing y campañas de concientización al personal.

EN RESUMEN:

Los ciberdelincuentes han perfeccionado el arte del engaño. No basta con tener antivirus o un buen celular, sino que ahora el escudo más fuerte es tu criterio.

Desde Cavecom-e seguimos comprometidos con promover una Venezuela digital más segura, consciente y protegida.

Richard Ujueta
Presidente



Erick Beni
Vicepresidente

Rafael Núñez
Director de Ciberseguridad Nacional

institución:contacto@cavecom-e.org.ve