Banesco ofrece charlas informativas antifraude a clientes del CC Metrópolis

El curso denominado Mejores Prácticas del Tarjetahabiente en Cajeros y Puntos de Venta está diseñado para educar al personal de los comercios afiliados, clientes y nómina interna del banco. Prestar atención es una de las principales claves para evitar ser timado con alguno de los modus operando usados por las bandas organizadas

Caracas.-

En los próximos días, Banesco Banco Universal realizará una serie de charlas informativas sobre las mejores prácticas para mitigar el fraude con tarjetas de crédito y de débito a los responsables de las tiendas y locales del centro comercial Metropolis, ubicado en Valencia, estado Carabobo.

El curso denominado Mejores Prácticas del Tarjetahabiente en Cajeros y Puntos de Venta, está diseñado por la Coordinación de Capacitación y Desarrollo en TDC/TDD, adscrita a la Gerencia de Prevención y Control de Fraude. La Coordinación fue creada en noviembre de 2002 con el propósito de educar y actualizar al personal de los comercios afiliados, a los tarjetahabientes y a la nómina interna sobre las mejores prácticas en el proceso de aceptación de tarjetas y del tarjetahabiente en cajeros automáticos y puntos de venta.

Si no se está atento, cualquiera puede ser víctima de las bandas organizadas o personas dedicadas al fraude con tarjetas de débito o crédito. Uno de los modos de operar más comunes es el llamado cambiazo, que puede darse en el cajero automático (una persona le advierte que está usando mal el cajero y se ofrece a enseñarle cómo hacerlo, pero una vez que marca la clave el cliente es distraído y le sustraen la tarjeta) o en un punto de venta (se produce con la complicidad de un empleado del local, quien cambia el plástico por otro parecido).

Está también la llamada manipulación, que requiere la participación de al menos 3 delincuentes. Cuando la persona introduce la clave, uno de los ladrones la copia en un papel. En ese momento, otro de los delincuentes le advierte al cliente que el cajero no entrega efectivo y que se cambie al otro ATM, cuando la persona desliza su tarjeta le indican que el otro cajero está dispensando el efectivo. Uno de los delincuentes aprovecha entonces para introducir la clave y debitar los montos de la cuenta del cliente timado.

Uno de los fraudes que ha tomado mayor auge en los últimos años es la clonación (skimmin, en inglés), que consiste en copiar la información de la banda magnética de una tarjeta auténtica para llevarla a otras tarjetas con propósitos ilícitos, esto ocurre en segundos y los equipos necesarios son de pequeño tamaño, incluso pueden ocultarse en un bolsillo. Los dos escenarios más comunes en los que se produce la clonación son con la complicidad de un empleado de un comercio que aprovecha el descuido del cliente o por medio de la incorporación de dispositivos a un cajero electrónico que permitan la clonación y hasta la grabación del momento en que la persona introduce la clave secreta.

En ese sentido, se recomienda al cliente no perder de vista la tarjeta al momento de cancelar; cerciorarse de que nadie observa cuando introduce la clave secreta y no decirla en voz alta; no aceptar ayuda de terceros; no realizar operaciones en cajeros que presenten alteraciones físicas y oprimir la tecla CANCELAR cuando termine cualquier operación. Si requiere hacer una llamada al Centro de Atención Telefónica no permita que otros le faciliten un celular o realicen la llamada por usted, hágalo usted mismo.

En el caso de las tarjetas de crédito la delincuencia organizada una de las principales modalidades es el robo del plástico. El más común es cuando la persona es víctima de un atraco o hurto y el ladrón se hace de las tarjetas y los documentos de identidad del cliente, con los que posteriormente realiza compras o cargos en establecimientos.

Otro de los modus operando es aprovechar un descuido del cliente al momento de pagar para sustituirle la tarjeta verdadera por otra. Asimismo, si el delincuente logra tener acceso a la información personal del cliente –nombres y apellidos, lugar y fecha de nacimiento, número de cédula de identidad, dirección de habitación, dirección de trabajo, números de cuenta y números de tarjetas– los usa para contactar a los comercios vía telefónica, por correo e internet.

Pero, si bien es importante que el titular del plástico esté atento a cualquier irregularidad cuando usa este medio de pago, también es necesario que el personal de los comercios afiliados se apegue a las mejores prácticas para evitar ser sorprendido por los delincuentes.

La persona encargada del punto de venta debe solicitar además de la tarjeta, la cédula de identidad laminada o el pasaporte para verificar que se trata efectivamente del titular. Asimismo, tomar nota de cualquier actitud sospechosa al momento de pago.

En el punto de venta debe ingresarse los últimos cuatro dígitos de la tarjeta, el código de seguridad que aparece en la parte posterior del plástico junto a la firma y el número de cédula del documento. Hasta que finalice la aprobación de la operación, el representante del local debe mantener los documentos y observar los componentes o características de seguridad de la tarjeta para certificar que es auténtica. En el caso de sospecha sobre la tarjeta o el tarjetahabiente, puede activar por seguridad el código 10 con el banco al cual corresponda el punto de venta.