FRAUDES INFORMÁTICOS Y ALERTAS QUE DEBEN TENER LOS USUARIOS RESPECTO A SU CONFIDENCIALIDAD

Los Fraudes Informáticos son aquellos que se efectúan por una o varias personas externas a la entidad financiera para obtener algún beneficio de quien sí es cliente. También roban los datos personales, clave, contraseñas y demás mientras se realiza una transacción por internet.
Veamos cómo identificar algunos de estos fraudes:

1) PHISHING - ¿Qué es el Phishing?

Es un fraude o delito informático, a través del cual se obtiene información personal (claves, usuarios o coordenadas) mediante correos electrónicos falsos.

¿Cómo reconocer si un correo es falso?

- Le pueden solicitar datos personales, financieros y que actualice sus datos en línea. Una característica es que le ofrecen premios.
- Los correos los envían con títulos de asuntos/subject de: “Pedido Urgente” indicando que su cuenta podría ser cerrada si no confirma, verifica o coloca su información de forma inmediata.
- Una característica muy común en la que hay que fijarse es que a menudo contienen errores ortográficos y de redacción.

2) SKIMMING - ¿Qué es el Skimming?

El denominado Skimming es la modalidad de fraude de alta tecnología mediante el cual se usan dispositivos electrónicos que son insertados y acomodados físicamente por los delincuentes en un cajero automático de una entidad financiera, para capturar los datos de la banda magnética de una tarjeta de crédito o débito de manera fraudulenta. Estos datos son luego insertados en una tarjeta falsa.

Consejos

- Trate de utilizar cajeros automáticos de la entidad financiera en donde tiene cuenta.
- Antes de introducir la tarjeta en el cajero automático, verifique que no tenga ningún dispositivo sospechoso, ajeno al mismo ni nada sobrepuesto.
- Si no hay protección en el teclado del cajero, cubra con su mano el teclado al ingresar su clave.

3) CAMBIAZO - ¿Qué es el cambiazo?

El cambiazo ocurre cuando un desconocido solicita su ayuda o intenta realizar transacciones en un cajero automático. Esta persona solicita su tarjeta usando excusas como el intentar limpiarla o revisarla, y durante un momento en el que el dueño de la tarjeta se distrae, cambia la tarjeta por otra.

Consejos

- Cuando reciba una nueva tarjeta de su entidad financiera, fírmela y averigüe bien dentro de la entidad cómo utilizarla.
- Nunca pida o acepte ayuda de desconocidos.
- Utilice su cuerpo como una barrera visual al momento de ingresar su clave. No deje que nadie se acerque a ver lo que hace.
- Luego de realizar cualquier transacción, verifique siempre su nombre en la tarjeta.

4) SUPLANTANCIÓN DE EMPLEADOS - ¿Qué es la suplantación de empleados?

Esto ocurre cuando alguien se hace pasar por un empleado del Banco, ofreciéndole agilitar un depósito. Esta persona solicita el dinero del cliente y lo hace esperar en algún lado, para luego desaparecer con el dinero una vez que el cliente se haya distraído.

Consejos

- Nunca divulgue sus movimientos financieros.
- Solo el personal que se encuentra en ventanilla está autorizado a recibir los valores a depositar. No entregue su dinero en lugares diferentes a las cajas.
- No permita que personas desconocidas se acerquen a la ventanilla en el momento en que le corresponda a usted realizar su operación.
- Si va a realizar retiros de dinero por montos altos, hágalo acompañado de otras personas o solicite el apoyo de la Policía Nacional.
- Deposite el dinero en efectivo solo en las ventanillas destinadas para ello. Los empleados del Banco jamás le solicitarán que lo realice en un sitio distinto a las ventanillas.