ROBO DE DATOS EN TARJETAS DE DEBITO

Cada día son más las personas que son estafadas en cajeros automáticos y con el avance de la tecnología los métodos son más sofisticados.

Existe desde la posibilidad de estar ante un cajero automático "ficticio" hasta la posibilidad de que se haya puesto una cámara oculta para grabar la operación.

Se estima que en Argentina el 60% de los fraudes con tarjetas se debe a la clonación de los plásticos y al uso no autorizado de las cuentas, un 33% está relacionado con el robo o la pérdida del plástico y un 7% a otros tipos de fraudes informáticos.

La ventaja de la tarjeta de débito respecto a la de crédito es que la primera solo permite extraer o gastar dinero mientras que haya saldo disponible en la cuenta y muchas tienen un límite diario.

COPIA DE DATOS

Se coloca un lector de tarjetas en el cajero que tiene una apariencia similar al que se usa para abrir la puerta.

El usuario utiliza su tarjeta para retirar dinero, consultar saldos, ver sus últimos movimientos, etc. Al pasar la tarjeta por este lector se copian los datos de la banda magnética. La clave de la tarjeta es obtenida a través de una cámara oculta que enfoca el tablero o touchscreen del cajero automático. La filmación es enviada en forma inalámbrica a los delincuentes quienes normalmente se encuentran en un radio no mayor de 100 metros con alguna computadora portátil que recibe estos datos.

Una vez obtenidos el número de tarjeta (copiado de la banda magnética) y la contraseña del usuario se pueden duplicar las tarjetas las cuales generalmente son usadas en forma inmediata antes de que el titular de la misma denuncie a su banco emisor el faltante de dinero.

REPLICA DE CAJEROS

El usuario al intentar realizar su transacción recibe un mensaje en pantalla de "operación cancelada", extrae su tarjeta y se retira.

La víctima realmente ha ingresado sus datos en una réplica de cajero que ha sido utilizada sobre la real (touchscreen, teclados y lector de banda magnética). Luego los estafadores desmontan sus equipos obteniendo de esta manera los datos bancarios de la víctima.

“LAZO” o “LAZO LIBANES”

En este caso se introduce en la ranura del cajero un trozo de placa de rayos x en forma casi imperceptible provocando de esta forma que el cajero no reconozca a la tarjeta o la reconozca a medias.

Al encontrarse con que el cajero no devuelve el plástico, el estafador intenta ayudar a la víctima indicándole que ingrese nuevamente la contraseña. Como esta posibilidad tampoco provoca la expulsión del plástico, la víctima se retira y el estafador obtiene la tarjeta y su clave.

RECOMENDACIONES

Al crear su contraseña o clave no la vincule con datos personales (fecha de nacimiento, DNI, patente de su vehículo, número de teléfono, cumpleaños de hijos, conyuge o padres), etc.
Memorice su clave y no la revele a persona alguna.
Al utilizar un cajero automático verifique que éste no presente imperfecciones en sus bordes (de la pantalla, del slot en que ingresa la tarjeta, del teclado, etc). Si observa una irregularidad de estas características, no utilice ese cajero en particular.
Siga las instrucciones que le brindan por pantalla.
No converse con extraños que estén cerca suyo en el cajero.
Guarde el recibo emitido ya que el mismo tiene información de su cuenta (y en muchos casos el número de cuenta bancaria completo)
Cuando termine de extraer dinero, teniendo el plástico y el comprobante en su poder, verifique que la pantalla se encuentre emitiendo la misma información que usted vio antes de ingresar su tarjeta.
ADECUA (Asociación de Defensa de Consumidores y Usuarios de la Argentina) aconseja cambiar los códigos de las tarjetas cada tres meses.

Luciano Salellas
Auditor en Seguridad Informática

Miembro de GARP (Global Association of Risk Professionals)
Consultor en SR HADDEN SECURITY CONSULTING y
RISK INFORMATION ADVISORS
MATR. APPEI 339

http://www.sr-hadden.com.ar