La claridad del comisario Elisio Guzmán Cedeño

Clonaron a la oveja Dolly... ¡Las tarjetas son falsificadas!

¿Cuál es la diferencia entre la clonación y la falsificación? La clonación puede definirse como el proceso por el que se consiguen copias idénticas de un organismo ya desarrollado, de forma asexual. Estas dos características son importantes. Se parte de un animal ya desarrollado, porque la clonación responde a un interés por obtener copias de un determinado animal que nos interesa, y sólo cuando es adulto conocemos sus particularidades. La falsificación es un acto consistente en la creación o modificación de ciertos documentos, efectos, bienes o productos, con el fin hacerlos parecer como verdaderos, o para alterar o simular la verdad.

Esta entrada sirve para explicar la exactitud del delito informático conocido popularmente como "clonación de tarjetas de débito y tarjetas de crédito". El comisario Elisio Guzmán Cedeño aclara que no es purista del lenguaje, pero un amigo le dijo con sencillez "Clonaron a la oveja Dolly, las tarjetas las falsifican". Así inició su participación en la III Conferencia Internacional Delincuencia Organizada y Derechos Humanos.

¿Cómo se lleva a cabo la falsificación de tarjetas? El ex director del Cuerpo Técnico de la Policía Judicial lo resume en la expresión "robo de identidad", a través de los métodos utilizados por la delincuencia organizada para la comisión de este grave delito.

- Se recogen extractos e información sobre datos personales directamente de la basura (informática).
- Puede ocurrir el robo de correspondencia de los buzones, para obtener tarjetas de crédito, estados de cuenta, ofertas personalizadas, datos del seguro social, Seniat, entre otros.
- El delincuente puede acceder a informes de crédito de forma fraudulenta, haciéndose pasar por empleado de la banca o de una empresa contratada por la entidad financiera.
- Además puede obtener datos personales, cédula de identidad, Seguro Social.
- Asimismo, espiando en los cajeros para identificar el numero PIN tecleado.
- A través del correo electrónico, envía mensajes simulando ser una comunicación oficial del banco y solicita datos de confirmación, como el número de la tarjeta de crédito o de débito y la clave.

- El ex director general del antiguo Cuerpo Técnico de la Policía Judicial pide instaurar una verdadera cultura de la seguridad en la organización financiera. "Hay que involucrar a todos los miembros del equipo, tratar la seguridad como un aspecto estratégico para el negocio y dejarla en manos de expertos"

El ex director general del antiguo Cuerpo Técnico de la Policía Judicial pide instaurar una verdadera cultura de la seguridad en la organización financiera. "Hay que involucrar a todos los miembros del equipo, tratar la seguridad como un aspecto estratégico para el negocio y dejarla en manos de expertos"

- Todos los miembros de la organización, desde el director general hasta el último trabajador, así como los clientes, proveedores y todo aquel que tenga acceso a los sistemas de información deben recibir formación en materia de seguridad

Clonaron a la oveja Dolly...

Comisario Elisio Guzmán Cedeño ex director del Cuerpo Técnico de la Policía Judicial.

Asegura el experto policía que "la mala utilización de los recurso tecnológicos, adaptándolos a las necesidades menudas del ciudadano común ha hecho que se desvirtúe el uso de algunas herramientas".

Citó un caso recientemente ocurrido en la provincia de Venezuela donde se utilizaron las tarjetas de débito como instrumentos de crédito, las cuales eran entregadas al agiotista (usurero, prestamista), suministrándole la clave y dejándolas en prenda hasta que la nómina se hiciese efectiva.

–Lo que luego ocurrió fue que se hicieron retiros por más de lo pactado y posteriormente se pretendió que el Banco reconociera la pérdida aduciendo el desconocimiento del retiro o en todo caso no haber realizado la operación.

Creemos –plantea- que nunca serán muchos los esfuerzos por generar en el público en general una responsabilidad en el uso de las claves, no sólo en el área bancaria sino también en todo lo atinente a la protección de la identidad y su seguridad en general.

Otro caso involucró al personal interno de una institución bancaria, "en la que un empleado desleal de una importante instancia tecnológica, copió, obviamente, de manera ilegal, importante información de los clientes y los códigos que permitían desencriptar esa información. Logró asignar y reasignar claves, utilizando una computadora portátil. "Así fue falsificando una importante cantidad de tarjetas perfectamente reconocidas por los cajeros de cualquiera de las redes. Con una máquina lectograbadora e información de los números de cuenta que había obtenido, tomaba cualquier tarjeta (había una de un cyber) y le grababa los números de cuenta. Si la tarjeta todavía no tenia pin (clave), le grababa una y extraía el dinero que el titular pudiera tener en la cuenta. Operó durante un tiempo y hubo que montar todo un largo operativo de análisis e investigación para contrarrestarlo.

Recomienda a las instituciones financieras "afinar las herramientas para las verificaciones de los datos suministrados durante los procesos de pre-empleo (ingreso de personal), además de comprobar fehacientemente la lealtad de las personas ubicadas en todas las áreas de las instituciones, pero con mayor énfasis en las que manejan procesos tecnológicos sensibles.

RECOMENDACIONES

● El comisario Elisio Guzmán asevera que las empresas financieras deben estar conscientes de que la seguridad es un aspecto crítico para el negocio. En nuestros días, el valor fundamental de una compañía son los activos intangibles. “Además, en determinados sectores, como la banca y el comercio electrónico, es necesario generar confianza en los consumidores y usuarios”.

● Pero hay más consejos para las instituciones financieras, de parte del experimentado investigador policial:

● Cuente los recursos destinados a proteger la seguridad de sus sistemas de información como una inversión, no como un gasto.

● Conozca sus debilidades. Encargue a profesionales especializados un estudio de vulnerabilidades de sus sistemas de información, tanto externos (hackers, troyanos…) como internos (mal uso de la información por parte de empleados o acceso de éstos a información confidencial).

● Actualice el software, antivirus y firewalls de su empresa.

● Vigile los accesos y el tráfico de información de sus sistemas informáticos.

● Relacionando todos esos datos entre sí –asegura–se pueden detectar intentos de acceso fraudulento o extracciones anómalas de información, y comprobar si efectivamente se trata de un intento de delito.

● Recomienda mantenerse atento a los movimientos sospechosos que puedan producirse en su entorno. “Los servicios de vigilancia digital permiten detectar el registro de dominios o sitios Web que intenten suplantar el nombre de la organización, copiar su home o utilizar fraudulentamente su marca”.

● Otro consejo es establecer una política clara de acceso a la información. “Ya sea a través de un sistema de claves o de cualquier otro, se debe definir claramente quién puede acceder a cada información y en qué condiciones”.

● Además, se debe poner marcha un plan de formación interna en materia de seguridad. “Todos los miembros de la organización, así como clientes, proveedores y todo aquel que tenga acceso a los sistemas de información deben recibir formación en materia de seguridad e implicarse en la tarea de mantenerla, desde el director general hasta el último trabajador”.

● Alguien que ha acumulado años al servicio de la seguridad no puede dejar de mencionar que la seguridad de la organización debe estar en manos de profesionales. “Sólo los expertos podrán analizar sus necesidades y ofrecerle lo que más le conviene, protegiendo sus sistemas de información y liberando al personal interno de esa tarea”.

● Por último, pide instaurar una verdadera cultura de seguridad en la organización financiera. Hay que implicar a todos los miembros del equipo, tratar la seguridad como un aspecto estratégico para el negocio y dejarla en manos de expertos”.