Robo de identidad

En un mundo cada vez más globalizado y tecnificado nos exponemos diariamente a decenas de situaciones que vulneran o comprometen nuestra identidad. Aun sin percatarnos podríamos ser víctimas de robo de información crítica o sensible, como por ejemplo nuestros números de cuenta bancaria o tarjetas de crédito, domicilio personal o quizá nuestro número telefónico, y utilizarlos para cometer alguna fechoría. Lo anterior es parte de un acto ilícito denominado "robo de identidad".

De acuerdo con el Departamento de Justicia de los Estados Unidos, el robo de identidad es un crimen que consiste en la obtención ilícita de información personal de un individuo y emplearla para cometer actos fraudulentos o de engaño, generalmente para conseguir un beneficio económico.

El robo de identidad no es reciente; sin embargo, en los últimos años los delincuentes se han apoyado cada vez más en la tecnología, sobre todo cuando se trata de obtener información financiera. Para ello, existen distintas técnicas, entre las que figuran:

Phishing. Consiste básicamente en enviar correos electrónicos de manera masiva con información que hacen pensar al usuario que proviene de páginas confiables (generalmente instituciones financieras u organizaciones serias), pero cuyo contenido posee vínculos a páginas falsas que buscan obtener de forma ilícita información confidencial.

Pharming. Se envía un correo electrónico a la posible víctima y al abrirlo se instala un *malware* que altera el contenido de ciertos archivos del sistema, de tal forma que al intentar acceder a páginas web, por ejemplo de un banco, la redirige hacia portales fraudulentos sin que el usuario se dé cuenta de ello.

Dumpster diving. Es una técnica empleada por los delincuentes que consiste en hurgar en los botes de basura y recolectar información, ya sea personal o de alguna empresa: estados de cuenta bancarios, tarjetas de crédito o débito, nombres, direcciones, teléfonos, suscripciones, recetas médicas, promociones; es decir, cualquier documento que permita conocer con mayor profundidad a la virtual víctima.

Clonación. Consiste en utilizar un dispositivo denominado *skimmer*, que duplica la información contenida en una tarjeta bancaria. Los malhechores instalan hábilmente estos aparatos en cajeros automáticos sin que los usuarios lo noten a primera vista. Cuando se desea sacar dinero, la tarjeta se introduce en la ranura del cajero sin saber que previamente es leída por el skimmer. Algunos delincuentes son tan sofisticados que incluso colocan cámaras de video cerca del teclado para grabar el NIP de la víctima, o enciman plantillas idénticas a los teclados para registrar esta clave. En los restaurantes o establecimientos comerciales es más sencillo, pues cuando los clientes van a pagar, se llevan la tarjeta a una terminal alejada de su vista, la deslizan sobre el *skimmer*, y obtienen así la información deseada, y finalmente realizan el cargo como si nada hubiera ocurrido.

Desafortunadamente el robo de identidad está creciendo no solo en países como Estados Unidos o Canadá. El boletín emitido por el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (InfoDF) sitúa a México entre los diez primeros lugares en robo de identidad a nivel mundial, lo que representa pérdidas anuales por más de 108 millones de pesos. Debido a lo anterior y dado que cualquier persona puede ser víctima de este delito, es necesario tomar medidas preventivas que disminuyan el riesgo de caer a merced de estos delincuentes:

- Nunca abrir ligas de supuestas instituciones bancarias contenidas en correos electrónicos, en especial cuando es solicitada algún tipo de información personal. Mejor utilizar su dirección web oficial escribiéndola en la barra de direcciones del navegador.
- Eliminar correos electrónicos de remitentes desconocidos, sobre todo de aquellos que ofrecen promociones o regalos, ya que podrían contener un código malicioso capaz de dañar o robar información.
- Jamás realizar operaciones bancarias por Internet mediante el uso de computadoras de usuarios desconocidos o cibercafés; mejor utilizar equipos de cómputo confiables y libres de virus.
- Cuando se desechen estados de cuenta bancarios, propaganda con información personal, facturas, entre otros, destruirlos completamente rompiéndolos en pequeños pedazos, o bien triturándolos.
- Al realizar retiros o transacciones en cajeros automáticos verificar que la ranura donde se inserta la tarjeta no esté sospechosamente alterada y constatar que no haya objetos inusuales cerca o encima del teclado.
- Si se realizan pagos con tarjeta bancaria, ya sea en restaurantes o comercios, jamás perderla de vista y exigir que la terminal esté cerca del cliente.

La Comisión Nacional para la Defensa de Usuarios Financieros (CONDUSEF) sugiere

tomar las siguientes medidas en caso de que haya sido víctima de robo de identidad y los datos hayan sido utilizados para cometer algún fraude financiero:

1. Denunciar el delito ante el Ministerio Público.
2. En caso de que la tarjeta haya sido clonada, reportarla de inmediato a la institución bancaria correspondiente. Si esta no actúa, acudir a la CONDUSEF.
3. Presentar una aclaración ante el buró de crédito, en caso de que se haya alterado el historial crediticio como producto del fraude.

Llevar a cabo medidas preventivas siempre será la mejor opción para evitar estos delitos.

REFERENCIAS:

- CONDUSEF (2014). Conduguía, protege tu identidad, Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. Tomado de http://www.condusef.gob.mx/PDF-s/educacion_financiera/conduguias/conduguia-protege-tu-identidad.pdf.
- Department of Justice (2014). What are identity theft and identity fraud, U.S. Department of Justice. Tomado de http://www.justice.gov/criminal/fraud/websites/idtheft.html.
- InfoDF (2014). México, entre los diez primeros lugares en robo de identidad en el mundo, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal. Tomado de http://www.infodf.org.mx/web/index.php?option=com_content&task=view&id=1821&Itemid=217.