E-Business: Delitos tradicionales versus nuevas tendencias criminales

*Álvaro Morales Torres**
*Luis Valdebenito Guzmán***

Resumen

El presente artículo tiene por finalidad dar a conocer cómo el desarrollo de la ciencia afecta a la sociedad en su conjunto, sin hacer distinciones en las personas. En efecto, la tecnología telemática entrega un conjunto de herramientas a organizaciones criminales, las cuales obtienen un singular provecho de los avances de la ciencia, dando origen a nuevas conductas criminales que implican cambios en la forma de explotar comercialmente estos productos, así como en la legislación civil y penal de los estados.

Introducción

Con el desarrollo del "E-Business" o la lógica de hacer negocios por internet, cada día nacen nuevas empresas, productos y servicios en la red, con grandes ventajas respecto de la cantidad de público que los puede aprovechar, independiente del lugar físico donde estos se encuentren. Para efectos del medio de pago, la tarjeta de invitación no es otra que la tarjeta de crédito, para lo cual sólo basta recalcular la moneda

* Ingeniero de Ejecución en Computación e Informática, Universidad de Santiago de Chile; Ingeniero Consultor en Seguridad Informática y Perito Judicial. Académico UCINF.
** Ingeniero de Ejecución en Informática, Universidad de Ciencias de la Informática; Ingeniero Consultor en Seguridad Informática. Académico UCINF.

de facto estándar —el dólar— a la moneda local. Desde luego que esta nueva forma de negociar es cada vez más común, sin embargo, es importante señalar que este sistema es débil en cuanto a su control y seguridad, ya que el anonimato que provee la red es muy favorable para aquellos inescrupulosos que quieren aprovecharse de la falta de certeza en la vigilancia automatizada de los compradores, facilitando la comisión de ilícitos, tales como estafas y usurpación e infracción a leyes específicas sobre la información. Esta crítica al sistema, pese a los esfuerzos para impulsar la nueva economía digital, se hace con responsabilidad y con afanes absolutamente constructivos. En relación a este análisis conviene hacer una clasificación de algunas conductas ilícitas, con el propósito de que el lector comprenda el objetivo que persiguen los autores de este trabajo.

1. Delitos tradicionales

1.1. Falsificación de billete

La falsificación de dinero es algo muy común hoy en día, es por eso que, por ejemplo, al entrar al local de un negocio, no es extraño ver un billete pegado en la vidriera de la caja de pagos con un timbre que diga "falso". Se puede observar cómo los llamados delitos económicos tradicionales se apoyan en las nuevas tecnologías informáticas. Hace algún tiempo se apreciaba a verdaderos artistas plásticos realizando algunas de estas falsificaciones, con herramientas que sólo ellos dominaban y de muy difícil acceso para adquirirlas. Además de la "expertís" de estos, para realizar estos ilícitos en la actualidad no se necesita de una especialización en la materia plástica o artística, el delincuente sólo requiere de muy pocos recursos: basta un simple escáner, un computador, una impresora de mediana calidad, un papel común y un programa de edición de imágenes, elementos con los cuales el delincuente podrá hacer múltiples copias de un billete, los que luego liberará dolosamente en el mercado.

Algunas falsificaciones ya más elaboradas requieren materiales de mayor calidad, de tecnología que el delincuente adquiere del extranjero —por ejemplo, a través de la misma red internet— y cierto tipo de papel, de similares características al que se

ocupa en nuestro país para la emisión de billetes. Luego, con un escáner de alta calidad, captura la imagen del billete a falsificar para digitalizar su "matriz". Mediante el uso de un computador y software especial de diseño, es posible retocar o mejorar la imagen, la que una vez perfeccionada sólo basta imprimir. Es así como en algunos casos se ha detenido a jóvenes intentando pagar a repartidores de pizza a domicilio con billetes recién elaborados en sus habitaciones.

1.2. Falsificación de instrumento privado mercantil

Clásicamente, los estafadores también explotaban las ventajas comerciales que otorgan los documentos privados mercantiles o cheques, los que obtenían abriendo una cuenta corriente con datos falsos, comprando cheques robados o adulterando alguno de estos documentos. No obstante las bondades de la tecnología actual, esta no hace distinciones en la sociedad, lo que implica que una parte de ella, la delincuente, ha sido beneficiada, específicamente en la simplificación y perfeccionamiento de su "modus operandi". De hecho, con las mismas herramientas señaladas en la falsificación de billetes, hoy resulta común la falsificación de talonarios completos de cheques, numerados en secuencia y con datos al gusto del consumidor, de acuerdo a sus preferencias: banco, nombre del propietario, número de cuenta y serie de los documentos.

Este método es más ventajoso que el clásico billete, ya que los montos a estafar pueden resultar infinitamente superiores, apoyados en el desconocimiento del común de las personas y cajeros del comercio tradicional e ineficiencia en detectar una perfecta falsificación.

2. Delitos no tradicionales

La forma de delinquir explicada en el párrafo anterior cabe dentro de la clasificación de los delitos tradicionales, pues la falsificación es un ilícito que va perdurando en el tiempo, pero así como las tecnologías informáticas avanzan, la comisión de los delitos también y es por eso que se puede apreciar cómo nace una nueva clasificación para estos. Los delitos no tradicionales son los que han nacido hace muy poco tiempo: ataques vir tuales a centros de tratamiento de

información, clonación de teléfonos celulares, estafas en el comercio electrónico y, entre otros, clonación de tarjetas de crédito.

2.1. Tarjetas

La mayoría de las personas a quienes se les menciona la tarjeta de crédito se hacen la idea de una tarjeta de plástico con una banda magnética que permite acceder a la posibilidad, por decirlo de una forma informal, de "comprar sin pagar", esto es, diferir el pago de lo que se adquiere, para ser cancelado posteriormente, brindando la sensación de haber consumido algo sin haberlo pagado. Los criminales que realizan estafas con tarjetas de créditos no tienen la percepción de la gran mayoría de las personas, ya que para realizar los ilícitos ellos no necesitan del "plástico", sino de los datos que este porta, como el número de la tarjeta, y en algunos casos su fecha de expiración. Cabe preguntarse por qué ciertas veces la fecha de expiración no les interesa. La respuesta es muy simple: existen sitios web en los cuales para comprar un producto o servicio sólo se necesita el número de la tarjeta. Algunos de estos delincuentes revisan los basureros de los bancos en busca de los mencionados números, los cuales aparecen en las boletas de estado de cuenta de las entidades financieras, algunas de las cuales optaron por ocultar, mediante asteriscos, los primeros números de la secuencia, dejando al descubierto los últimos cuatro dígitos. También existe otra forma de obtener los preciados números de una tarjeta de crédito y es la propia generación de los números, mediante un método muy sencillo: sólo se debe llevar a efecto un pequeño algoritmo que se explicará a continuación.

2.1.1. Algoritmo de codificación del número de tarjeta de crédito

La codificación del número de la tarjeta se realiza en tres pasos:

- Se multiplican por dos todos los dígitos de las posiciones impares y en aquellos mayores de 9 se suman los dos dígitos.
- Después de calcular los nuevos números de las posiciones impares se suman entre sí todos los dígitos.
- Si el resultado es múltiplo de 10 entonces el número de tarjeta es valido (resultado MOD 10 = 0).

Veamos un ejemplo con la tarjeta 4539 4512 0398 7356, de la cual queremos comprobar que es un número válido:

- Multiplicar por dos los números de las posiciones impares (4 - 3 - 4 - 1 - 0 - 9 - 7 - 5) y dejarlos con un solo dígito:

  4x2=8
  3x2=6
  4x2=8
  1x2=2
  0x2=0
  9x2=18 ⟶ 1+8=9
  7x2=14 ⟶ 1+4=5
  5x2=10 ⟶ 1+0=1

Como se aprecia, los últimos tres dígitos dieron más de 9, por lo tanto se suman entre sí.

- Luego se deben sumar los dígitos de las posiciones pares y los nuevos de las posiciones impares.

8+5+6+9+8+5+2+2+0+3+9+8+5+3+1+6=80

- Por último, 80 es múltiplo de 10, en consecuencia, el número de tarjeta es válido.

2.1.2. Ingeniería social

Otra de las formas de operar de los delincuentes a la hora de obtener los números de las tarjetas de crédito, es realizar una llamada telefónica a un cliente de las empresas que otorgan estos servicios, haciéndose pasar por un ejecutivo extraen información de la "víctima", dentro de la cual está, por cierto, el número de tarjeta de crédito.

Para aquellos sitios web que requieren la fecha de expiración de la tarjeta, los delincuentes se dirigen a tiendas comerciales pequeñas, restoranes, hoteles o ciertos moteles, con la finalidad de encontrar el vale de ventas, el cual se genera en una máquina que tiene en una placa en relieve los datos de la empresa; luego se calza la tarjeta de crédito en una ranura y encima de esta se coloca el vale de venta que, por tener la propiedad de ser autocopiativo, tiene impresos los datos de la empresa y los de la tarjeta de crédito, una vez que se pasa un pequeño carro de chequeo. Estos vales son extraídos de los basureros o se encuentran cerca de las cajas de pago.

En las figuras 1, 2 y 3 se pueden apreciar los vales de venta, en los cuales aparecen los datos de la empresa que acepta la compra con tarjeta de crédito y el número de esta,

la fecha de expiración y todos los datos del cliente. En la Figura 3 fue borrado el nombre de la empresa, nombre del cliente, números de la tarjeta y fecha de expiración, para proteger la integridad de los antes mencionados.

Fig. 1

Fig. 2

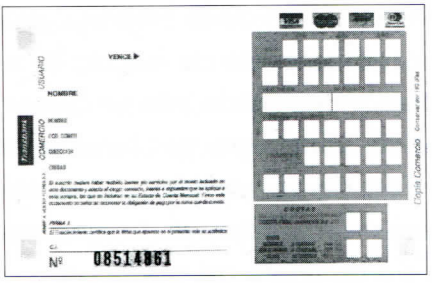
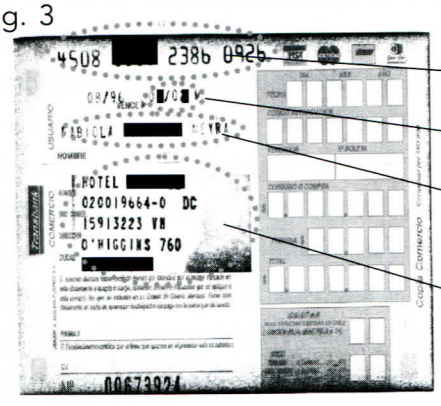


Fig. 3



Número de la tarjeta

Fecha de expiración

Nombre del titular

Datos de la empresa aceptante (nombre, código comercial, dirección y ciudad)

2.2. Clonación de tarjetas de crédito

2.2.1. Formato lógico

Para entender cómo se realiza la clonación de tarjetas de crédito, primero se debe conocer la estructura lógica de esta, es decir, los datos almacenados en su soporte magnético.

La grabación de la banda magnética de una tarjeta de crédito responde a una norma de la organización internacional de estándares (ISO), denominada Bank Identification Number (BIN), donde se sancionan las especificaciones técnicas de grabación para las pistas 1 y 2, ya que no se considera, para la gran mayoría de las tarjetas que circulan en el mercado nacional, la utilización de la pista 3.

En las pistas 1 y 2 se encuentran los siguientes datos:

a) Número de identificación (PAN-Primary Account Number)
Corresponde al número de identificación de la tarjeta que se halla en la impresión en relieve del anverso del plástico. El formato del campo PAN es BBBB PP RRRRRRRR M D, donde

BBBB : BIN asignado por la ISO a cada institución financiera
PP : Dos dígitos para uso del emisor de libre disponibilidad
RRRRRRRR : RUT del cliente
M : Número del miembro (0 = titular, 1-9= adicionales)
D : Dígito verificador del número de tarjeta

b) Nombres
Contiene el nombre del cliente a quien se le asigna la tarjeta, debiendo ser el mismo indicado en la impresión en relieve del plástico. El formato del campo de largo de 26 caracteres es el siguiente:

Nombres
Espacio
Apellido paterno
Espacio
Apellido materno
Separador (/)

Si los datos del nombre ocupan menos de 25 caracteres se debe ajustar a la izquierda y rellenar con blancos por la derecha hasta la posición 25. La posición 26 siempre debe contener un separador (/).

c) Fecha de expiración
Fecha de expiración de la tarjeta en formato AAMM, donde:

AA = Últimos dos dígitos del año de expiración
MM = Dos dígitos del mes de expiración

d) Designador de intercambio
Establece el dominio sobre el cual puede ser utilizada la tarjeta.

1 = Disponible
5 = Disponible sólo para intercambio en el país de emisión de la tarjeta
7 = No disponible para intercambio general
9 = Tarjeta de prueba

e) Código de servicio

Establece los códigos (autorizados por la ISO) de los servicios a los cuales puede tener acceso la tarjeta, en el rango 00 al 49, tales como:

01 = Sin restricciones
02 = No servicios en ATM
03 = Sólo servicios en ATM
10 = No avance en efectivo
11 = No avance en efectivo; no servicio en ATM
20 = Autorización positiva: todas las transacciones debieran ser autorizadas por el emisor
41 = Circuito integrado presente: sin restricciones
43 = Circuito integrado: sólo servicio ATM

f) Código del país

Indica el código asignado al país de emisión de la tarjeta, siendo 152 el código para nuestro país.

2.2.2. Formato físico

Si bien el formato externo de la tarjeta es sujeto a decisión de la institución que la emite, las tres primeras líneas de impresión están preasignadas como sigue:

Ya con estos conocimientos, los criminales obtienen los datos de los clientes de las entidades bancarias y mediante máquinas de lectura y grabado de códigos de banda magnética,

Para el caso de tarjetas para titulares:

Primera línea de impresión	:	PAN
Segunda línea de impresión	:	Nombre del titular

Para el caso de tarjetas para adicionales:

Primera línea de impresión	:	PAN
Segunda línea de impresión	:	Nombre del adicional
Tercera línea de impresión	:	Nombre del titular

O bien:

Primera línea de impresión	:	PAN
Segunda línea de impresión	:	Nombre del titular
Tercera línea de impresión	:	Nombre del adicional

graban la información en tarjetas vírgenes, mediante una computadora.

2.2.3. Obtención de claves de las tarjetas de crédito vía telefónica

No sólo basta con conocimientos del "negocio" más los datos obtenidos para realizar algún ilícito, sino que los delincuentes informáticos, en su constante afán de vulnerar los sistemas de tratamientos de información, buscan nuevas herramientas y métodos para su actividad delictiva.

Como estos criminales tienen gran conocimiento de las tecnologías informáticas, teóricamente no existen barreras que ellos no sean capaces de sortear. Por ejemplo, experimentando y probando nuevos programas han llegado a lograr la decodificación de los tonos generados por los aparatos telefónicos. Los delincuentes realizan llamadas telefónicas a los usuarios de las tarjetas de crédito y, mediante un discurso muy bien elaborado, en el cual, haciéndose pasar por administradores del sistema informático que controla las cuentas, solicitan a la víctima que digite su clave, correspondiente a la tarjeta de crédito en el equipo telefónico que porta, sin importar si es de red fija o móvil, pues lo único que les interesa es poder capturar los tonos que se generan al presionar los botones. Una vez con los tonos en su poder, estos son procesados mediante programas de tratamiento de sonido, logrando de manera muy sencilla decodificarlos y obtener los números asociados.

Entonces, ya con las *claves* en su poder, junto con las *tarjetas clonadas,* sólo les basta dirigirse a un cajero automático y completar su misión.

Conclusiones

Agradecemos frecuentemente a la comunidad científica que su constante investigación beneficie a la humanidad, como también a ingenieros y a técnicos por aplicar la ciencia, dando origen a diferentes tecnologías y otorgando una alto grado de avance en la modernidad. Sin embargo, vemos asombrados el accionar de organizaciones criminales altamente coordinadas, que sacan un particular provecho a estas nuevas tecnologías, que les permiten delinquir mediante el uso de diversos tipos de técnicas.

Hemos visto cómo, desde una perspectiva tradicional de delinquir, las bandas criminales actualizan sus metodologías asistidos, por cierto, en la tecnología, que no hace distinciones, para buscar novedosos "modus operandi". Ante ello, la ciencia aplicada no debe detener su actividad para evitar que los delincuentes se beneficien de ella, sino que deben ser creados mecanismos de control y seguridad para cada una de las actividades donde la delincuencia pueda perfeccionarse.

En el desarrollo de estas nuevas generaciones de delincuencia hemos comprobado, con mucha preocupación, que los tentáculos de las organizaciones criminales alcanzan no sólo a delincuentes comunes actualizados, sino también a algunos profesionales de la Ingeniería y estudiantes de estas carreras. Ello, por una razón muy simple: estas nuevas conductas criminales requieren un alto nivel de conocimientos técnicos para ser explotados a cabalidad.

Lo anterior nos lleva a una reflexión: es imprescindible no sólo educar a la sociedad en general que ocupa estos nuevos productos, sino, también, por parte de los establecimientos de educación superior, el incorporar valores, marcados fuertemente en la ética, a fin de que los futuros profesionales que formarán parte de este mercado, no sean tentados por estas bandas delictivas, las que, en definitiva, no lograrán destruir la tecnología, sino sólo sus esforzados años de estudios universitarios.