Robo de tarjetas al alza

Por las dificultades que implica castigar este delito así como por las altas de probabilidades de éxito que hay al cometerlo, el robo de datos bancarios se ha convertido en una de las prácticas favoritas de los criminales en México

NACIONAL

ROBO DE TARJETAS AL ALZA

#Fraude

Por las dificultades que implica castigar este delito así como por las altas probabilidades de éxito que hay al cometerlo, el robo de datos bancarios se ha convertido en una de las prácticas favoritas de los criminales en México

POR ERNESTO SANTILLAN

Cuando Patricia Sánchez terminó la llamada con quien creyó que formaba parte del personal del banco HSBC, el dinero de la jubilación que recibe mes con mes se había esfumado de su cuenta.

"Tardé como tres horas en darme cuenta que había sido una estafa. Fue hasta en la tarde que fui al supermercado y mi tarjeta no pasó que me 'cayó el veinte'.

"Me marcaron aproximadamente a las dos y media de la tarde, el número no lo tenía registrado pero no parecía extraño, estaba esperando un paquete de Amazon y por eso decidí contestar.

"En cuanto me dijeron que eran del banco pensé en colgar, pero inmediatamente comentaron que había problemas con mi cuenta y se refirieron a mí por mi nombre, lo que provocó que me dieran confianza y pues terminé entregando mis datos para que realizaran lo que supuestamente sería una verificación de mi cuenta".

La originaria de la Ciudad de México admite que sabía de este tipo de robos, sin embargo dice que eran casos lejanos y nunca imaginó que a ella le sucedería, pero aprendió la lección.

"No me vuelve a pasar, ahora sé perfectamente que los bancos nunca hacen este tipo de llamadas. Afortunadamente mi esposo también recibe su jubilación y con eso pudimos compensar el robo".

Datos del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP), revelan que tanto las llamadas de fraude como de extorsión se incrementaron desde el 2019, alcanzando su pico máximo durante el 2022, cifra que parece será superada al finalizar el año en curso.

Hace cuatro años, al inicio de la administración actual, el SESNSP contabilizó 2 mil 963 víctimas de este delito. Durante el 2020, la cifra bajó a 2 mil 832; un año después, volvió a subir a 2 mil 900 carpetas de investigación.

Desde entonces, la víctimas de estos delitos no han dejado de aumentar. En el 2022, se registraron 3 mil 558 casos y en los primeros cuatro meses de este año van 3 mil 473.

Innovación criminal

A las llamadas de extorsión y fraude se suma otro tipo de delito denominado "carding", el cual tiene el objetivo de obtener los datos de las tarjetas de crédito o débito sin tener que llevar a cabo el proceso de engañar vía telefónica o por correo electrónico a los usuarios bancarios.

Ante este panorama, el Instituto Nacional de Acceso a la Información y Protección de Datos Personales (INAI), lanzó una alerta en la que informa que los diversos métodos utilizados por los delincuentes para este fin.

"Una de las técnicas más usadas para obtener los números de las tarjetas, se denomina '*Shoulder surfing*'. En este caso, una persona simplemente mira disimuladamente el número de la tarjeta cuando se va a pagar y lo memorizan, al igual que el código de verificación.

"En las compras en línea suelen utilizarse tiendas falsas con ofertas que realmente no existen. Una vez que se ingresan los datos, los ciberdelincuentes se quedan con el número de tarjeta y el producto jamás llega", informó el INAI.

De acuerdo con el Instituto encargado de la protección de datos en el país, la información de las tarjetas es utilizada para realizar compras que no suelen ser muy grandes, sino cargos recurrentes como pagos de cuentas de *Spotify*, *Netflix*, *YouTube*, *Uber* o suscripciones mensuales a videojuegos, de manera que los importes sean pequeños y secuenciales, para evitar levantar sospechas y que sea difícil darse cuenta de que la estafa está sucediendo.

Jurisdicción poco efectiva

A pesar de que el Código Penal Federal contempla la extorsión, la impunidad en esta materia es muy alta.

De acuerdo con el artículo 390, al que sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro o causando a alguien un perjuicio patrimonial, se le aplicarán de dos a ocho años de prisión y de cuarenta a ciento sesenta días de multa.

De acuerdo con la legislación vigente, las penas se aumentarán "hasta un tanto más si el constreñimiento se realiza por una asociación delictuosa, por un servidor público, exservidor público o por miembros o exmiembros de alguna corporación policial o de las Fuerzas Armadas Mexicanas".

Pero sin importar las consecuencias, este fenómeno crece de manera constante en el país.

Según la propia Secretaría de Seguridad y Protección Ciudadana (SSPC), la impunidad se debe en gran medida a la dificultad para rastrear a quienes cometieron el delito, aunado a las pocas denuncias por parte de las víctimas.

Por este motivo, la SSPC advierte que esta forma de delinquir se ha convertido en una de las favoritas de los criminales en los últimos años en donde no solo la delincuencia ha aumentado, también las tecnologías de la comunicación.

"La extorsión telefónica se ha convertido en uno de los delitos favoritos de la delincuencia debido a que implica menor riesgo de ser detenidos y mayor probabilidad de obtener algún beneficio.

"Por lo tanto es fundamental identificar el número telefónico del que llaman antes de contestar y evitar proporcionar información personal o familiar, si se responde la llamada de algún número desconocido", dice la institución encargada de la seguridad civil en México.

A pesar de que el Código Penal Federal contempla la extorsión, la impunidad en esta materia es muy alta

A las llamadas de extorsión y fraude se suma otro tipo de delito denominado "carding", el cual tiene el objetivo de obtener los datos de las tarjetas sin tener que engañar a los usuarios bancarios

Prevenir el *carding*

Recomendaciones para evitar el robo de datos bancarios al pagar con tarjetas de débito o crédito

- Nunca perder de vista la tarjeta cuando se utilice de manera física para realizar pagos.
- Evitar que la persona que realiza el cobro digital tenga acceso al Código de Verificación o CVV.
- Verificar que las páginas donde se realizarán las compras en línea cumplan con el protocolo de seguridad: deben iniciar con "https" y mostrar la figura de un candado cerrado en la barra de dirección.
- No utilizar redes o computadoras públicas al momento de realizar compras.
- Activar alertas de los movimientos con tarjetas, para llevar un mejor monitoreo de la actividad y detectar cualquier movimiento inusual.
- Monitorear los estados de cuenta para identificar compras que no se hayan realizado, en caso de existir alguna, reportarla inmediatamente.
- Destruir completamente las tarjetas de crédito o débito que ya caducaron.
- Desactivar la opción NFC de los dispositivos móviles mientras no se use, ya que esta tecnología permite conectar dispositivos para el intercambio de datos.
- Utilizar las tarjetas virtuales que ofrecen los bancos para pagos online.
- Cuando se reciba una tarjeta en el domicilio, es importante revisar que el sobre esté completamente cerrado.
- Contar con un porta-tarjetas antirrobo.

*FUENTE: INAI