

La policía se declara impotente contra los timos bancarios 'online'

Yolanda V. A., gallega de 33 años, abrió Internet para ojear su cuenta bancaria y se llevó un disgusto terrible. Alguien le había sacado 3.252 euros y los había transferido a la cuenta de un desconocido en Madrid. Nerviosa, miró también la cuenta de sus padres, en la que ella tiene firma autorizada, y faltaban otros 18.000 euros. La policía identificó rápido al receptor de las transferencias, pero ya era tarde: el dinero estaba en Ucrania. En los bolsillos de una de las sofisticadas mafias que infectan con virus malignos virus miles de ordenadores y se apoderan de dinero de las cuentas on line.

[JOSÉ ANTONIO HERNÁNDEZ - El País](#) - Un informe de Delincuencia Económica de la Dirección General de la Policía, al que ha tenido acceso EL PAÍS, avisa de la eclosión de este tipo de saqueos. Y admite la impotencia policial para detener "a los autores intelectuales". Primero, por los sofisticados métodos que emplean y, segundo, por la dificultad de perseguirlos, ya que actúan desde países del Este, Asia y Sudamérica. No todas las víctimas tienen la suerte de Yolanda. Su banco, el Pastor, le repuso el dinero. "Vieron que yo nunca había realizado transferencias desde Internet y me lo devolvieron", señala Yolanda. Pero el banco no tendrá fácil recuperarlo.

La policía siguió el rastro del dinero y comprobó que a Yolanda le habían robado desde unos servidores de Internet, en Ucrania. Y que, fraccionado en siete transferencias, los cacos lo habían remitido a una cuenta de una sucursal del Banco Pastor en Madrid a nombre del ingeniero informático José Antonio C. Ch. Y que éste, a su vez, lo había transferido inmediatamente a Ucrania a través de la Western Unión y MoneyGram. José Antonio C. Ch. fue detenido. Pero los agentes, no sin recelo, tuvieron que dejarle libre con cargos. Aseguró que no creía estar haciendo nada ilegal. La policía asegura que no todos los intermediarios "son impolutos". Cuando se ven sorprendidos, simulan ser víctimas ellos también.

-¿No le pareció extraño que, a pesar de lo reglamentado que está el mercado bancario, le ofreciesen un trabajo consistente en tramitar transferencias de dinero mediante comisión?

-No sospeché nada. Creí que era un trabajo normal.

Yolanda sólo es una de las múltiples víctimas de lo que en la jerga policial se llama la estafa del scam, un fraude cuya ejecución requiere varias fases. La primera consiste en captar a intermediarios dentro del país en el que la mafia va a actuar. En chat, foros y por correo electrónico lanzan miles de mensajes ofreciendo un trabajo "fácil, cómodo y de succulentas ganancias". Exhiben fotos de personas, sonrientes, que cuenta cómo se han enriquecido. La mafia estudia muy bien a los aspirantes antes de seleccionarlos: domicilio, profesión, hijos... Jamás hay encuentros personales. Mantienen los contactos a través de correos electrónicos. Condición para obtener el trabajo: tener Internet las 24 horas, ser español y disponer de una cuenta bancaria legalizada. Le explican que su misión se ciñe a recibir dinero en su cuenta para que lo saque inmediatamente y lo remita sin demora a números de cuentas extranjeras que ellos le indican. Le ofrecen un sueldo mensual o comisiones de hasta el 10% del dinero que transfiera. Antes, le aseguran que no se trata de blanqueo de capitales, sino de un negocio rentable y legal. Y que las transferencias van a ONG extranjeras y que la mayoría procede de subvenciones públicas y privadas. Los cacos se inventan una empresa, cuyo nombre van cambiando para dificultar las pesquisas policiales. La que estafó a Yolanda se llamaba Maximus Consulting.

Captados los intermediarios, comienza la segunda fase de la estafa: obtener claves y contraseñas de usuarios de banca on line. Emplean varias modalidades: el phishing; es decir, el envío masivo de correos electrónicos que informan de un problema de seguridad en las claves del banco. Y que dirigen a una web que simula ser la de una gran entidad bancaria española. En realidad es falsa, calcada de la auténtica. Si coincide que el usuario que recibe el mensaje trabaja con ese banco y se cree el mensaje, está perdido, ya que le piden que introduzca su clave para solucionar el problema. Cuando lo hace, los mafiosos se apoderan de ella. Otra modalidad es el pharming, que "infecta indiscriminadamente con virus malignos miles de ordenadores". Es especialmente maquiavélica. Cuando el usuario escribe en la barra de direcciones de Internet el nombre de su banco, el navegador le conecta automáticamente con una web falsa que imita a la de su entidad bancaria. No logra realizar ninguna operación, pero los estafadores le copian la contraseña.

Ya con las claves en su poder, empieza la tercera fase: los estafadores, desde miles de kilómetros, le sacan enseguida el dinero y lo transfieren a cuentas de los intermediarios, que tienen orden de estar muy atentos para ir rápidamente a su banco, sacar el dinero en líquido y remitirlo al extranjero.

La policía asegura en su informe que muy pocas veces se logra inmovilizar el dinero antes de que salga de España. Los intermediarios, conscientes o no de la ilegalidad, sí quedan a merced de la policía, pero "los autores intelectuales" salen impunes: actúan desde países "con un grado bajo de cooperación judicial-policial internacional", señala el informe. Y añade que pocas veces los jueces españoles acceden a enviar comisiones rogatorias a esos países. Y cuando lo han hecho por tratarse de sumas de dinero muy elevadas y de organizaciones delictivas de alto nivel, "el resultado ha sido prácticamente nulo". A ello se une que cada juzgado, a pesar de tratarse "de una estafa de ámbito nacional", suele llevar sus casos de forma individual y no hay constancia de que se inhiban "a la Audiencia Nacional".

Los agentes admiten que, agotada la búsqueda del dinero en España sin éxito, suelen "archivar" las investigaciones sin haber podido recuperarlo.

Fecha artículo: 2008-11-10 09:39:52 - url artículo: <http://www.internautas.org/html/4428.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org