LUN

Fecha: 09/01/2026 Audiencia: 271.020 Sección: ACTUALIDAD
Vpe: $3.195.579 Tirada: 91.144 Frecuencia: 0
Vpe pág: $4.399.200 Difusión: 91.144
Vpe portada: $4.399.200 Ocupación: 72,64%

Expertos en ciberseguridad explican cómo los delincuentes obtienen datos personales para hacer estafas

"Que una empresa te pida una foto del carnet por ambos lados, mostrando la foto, es una aberración"

Jefe de la PDI dice que la clave en las estafas telefónicas es la calidad de la información que manejan los delincuentes. "Les permite generar confianza con la víctima", dice.

A la actriz Amparo Noguera le robaron $700 millones con una elaborada estafa. Los delincuentes sabían hasta el estado de sus tarjetas bancarias.

JUAN MORALES

Todos somos generales después de la batalla y cuando nos enteramos de alguien que cayó en una estafa, en un cuento del tío, todos somos súper inteligentes y despiertos y comentamos pero cómo esta persona fue a caer en un engaño tan burdo. Pero como dicen por ahí, o como dice el subprefecto Gabriel Castro, el mismísimo jefe de la Brigada de Delitos Económicos de la PDI, nadie está libre.

A la actriz Amparo Noguera le sustrajeron 700 millones de pesos tras recibir una llamada de un tipo que se identificó como ejecutivo bancario que le advirtió que unos ciberdelincuentes estaban tratando de robarle su dinero desde sus cuentas bancarias. Por supuesto, hay gente confiada que es más propensa a caer, pero la clave en este caso, explica el subprefecto Castro, es la calidad de la información que manejaban los delincuentes.

"Porque la calidad de la información les permite generar confianza con la víctima", dice.

En este caso, sabían no sólo el número de teléfono de Noguera, su dirección, su RUT, sino también el banco del que era cliente, el estado de sus tarjetas de crédito y débito, y los montos y cupos que había en cada una de ellas. "Entonces, las víctimas le creen al tipo con quien están hablando y desconfían de todos lo demás", dice el PDI.

Todo esto sazonado con un ritmo frenético de urgencia, de que hay que actuar rápido para no darles tiempo a los delincuentes, cuando lo que buscan en realidad es no darle tiempo a la víctima para que se detenga a pensar, para que siga con la guardia baja.

¿De dónde sacan tanta información los delincuentes? ¿Dónde la obtienen, cómo la obtienen, quién se las pasa?

Fuentes abiertas. El ingeniero informático Héctor Moyano, que ha sido consultor en ciberseguridad para la Presidencia de la República y el Senado, explica que existe un montón de fuentes abiertas que los delincuentes utilizan para obtener datos.

En redes sociales, dice, hay gente que pone sus nombres y apellidos, suben fotos de sus autos, de sus casas. Son un libro abierto.

"Hay formas de hacer cruces de estas fuentes abiertas, usando incluso inteligencia artificial", dice. "Entonces con estos datos yo voy al mercado ilegal, en foros clandestinos, y vendo paquetes de información, donde tengo todos los datos de, por ejemplo, Juan Morales: su teléfono, su foto, su rut, su dirección, el nombre y foto de su esposa, su auto cero kilómetros, etcétera".

> **"El carnet contiene información crítica, no solo por el RUT"**
> Héctor Moyano, experto en ciberseguridad

Traspaso de datos. Un sistema muy generalizado de tráfico de datos es cuando ciertas empresas traspasan o venden la base de datos de sus clientes a otras empresas. "Pasa mucho con los call center", explica Sebastián Rebolledo, uno de los directores de 8.8, que organiza uno de los encuentros más importantes de ciberseguridad en Chile. "Estos datos los venden y los traspasan de un lado a otro".

De primera fuente. Otras veces, explica Moyano, somos nosotros mismos los que entregamos información personal. "Hay veces que ciertas instituciones nos piden, para ciertos trámites, que les mandemos una foto del carnet de identidad por ambos lados. Que una empresa te pida una foto del carnet por ambos lados, mostrando la foto, es una aberración; ninguna institución debería pedir algo así", sostiene.

"El carnet", agrega, "contiene información crítica, no solo por el RUT, sino por el número de documento (con el que se pueden hacer un montón de trámites notariales, por ejemplo), y en el reverso hay un código QR que remite los mismos datos que están en la cara principal del carnet. Y está la barra de números, que también contiene información importante".

Moyano recomienda, por último, mandar la foto del carnet ocultando toda la información que pueda ser usada para estafas.

Otra técnica que usan los delincuentes, explica el subcomisario Castro, es realizar llamadas para obtener información. "Por ejemplo", dice, "llaman y preguntar por Juan Pérez. No, equivocado. Y con quién hablo. Con Juan Morales. Ah, muchas gracias. Y cortan. Pero ya tienen el número asociado con un nombre. Luego llama otro y preguntan por el hijo o la esposa. Y así van juntando más datos. Y cuando reúnen suficiente información, hacen la llamada en serio para estafar".

La filtración. El subprefecto Castro dice que una de las hipótesis que se maneja en el caso de la estafa a Amparo Noguera, es que un empleado o ex empleado bancario haya filtrado o vendido información de los clientes.

"Otras veces", explica Moyano, "un ex trabajador de una empresa cualquiera se va con toda la base de datos y la hace circular".

Hackeo. Más sofisticado, aunque no por eso poco frecuente, es el hackero de instituciones públicas y privadas. Rebolledo recuerda que el 31 de diciembre pasado unos hackers revelaron miles de datos sensibles de pacientes de la Clínica Dávila, luego de que la clínica se negara a pagar una cuantiosa suma para que no lo hicieran.

También han robado computadores de reparticiones públicas con información vital, como la que sufrió hace un par de años el Ministerio de Desarrollo Social, que contenía datos de miles de personas.

"Y cuando te roban el celular, tú no sabes qué información obtuvieron, aparte de robarte el aparato", dice Moyano. "Incluso la información que las empresas guardan en la nube, están expuesta a hackeo y muchas veces lo hacen".