



## Los Datos Personales de todos los ciudadanos con CUIT y CUIL fueron expuestos

Por culpa de las serias fallas de seguridad y desactualización del sitio de datos de Seguridad Social del Gobierno.

En variadas plataformas y medios diferentes expertos en informática y seguridad señalaron graves fallas del sitio de **Procrear** que permitió, de forma muy irresponsable, **acceder a los datos de CUIT y a la contraseña de trámite** de todos los usuarios a través de una base de datos recopilada por Anses.

Es importante recalcar y desmentir un error que se propagó por varios medios y que también circuló por las redes: nadie "hackeó" nada. Simplemente, el sitio del Estado presentaba fallas relacionadas con la seguridad y problemas conocidos hace ya 9 años y los errores nunca fueron arreglados ni se habló del tema hasta hace una semana. Guido Vilariño, Ingeniero en sistemas de información por la Universidad Tecnológica Nacional, miembro del Observatorio de Derecho Informático Argentino y CoFundador de DemocracyOS, nos brinda mas información sobre el tema.

"La comunidad de seguridad informática sabe de esto hace mucho tiempo, y tengo entendido que hace mucho vienen avisando de estos problemas, pero nadie se calentó hasta que se empezó a hablar del tema hace poco. Si alguien "hackeara" el servidor del Ministerio del Interior, violaría el artículo 153 bis del Código Penal, o si un funcionario dejara expuesta información privada violaría los artículos 157, 157 bis y 249 del Código Penal. Y por más interesante que parezca hablar de un posible Mr. Robot argentino, éste no fue el caso.

"El sistema estaba configurado para servir cualquier dato que vos le pidieras. Al ser una página web, (URL) vos a la dirección le pedís que te dé cierta pagina con el CUIT y listo, te daba los datos de esa persona. y cuando hablamos de dato hablamos de **nombre completo, DNI, dirección de tu casa**, y si bien el sistema no permitía saber el sueldo de alguien, **como exponía el número de trámite del ANSES, con eso podías crear o cambiar tu clave de seguridad social o tu clave fiscal**, que en definitiva también te habilita a ver tu sueldo y aportes, entre otras cosas", nos explica el especialista.

No había absolutamente nada que bloquee o que de alguna manera restrinja el acceso a estos datos, estaban públicos a todo Internet. **No era necesario ningún hack, ni un programa especial.** Desde cualquier navegador, escribías la dirección y encontrabas el dato que querías.

Es muy fácil para una persona con muy pocos conocimientos en programación hacer un programa que vaya pidiendo los datos de los DNI uno por uno, que se incrementan y se guardan; y en cuestión de horas podría obtener los datos "privados" de todos los ciudadanos de Argentina. El sistema no hacía nada para prevenirlo: no había ni un Captcha, que es la medida más básica de seguridad. Mas allá de las vulnerabilidades: usaba una versión antiquísima de Ubuntu, tenía una versión vieja del servidor web, versiones viejas que algunas hace 9 años no se actualizaban. Al no tener Captcha y todo lo relacionado con seguridad, a un atacante si le permitiría explotar y robar esos datos. Pero acá ni siquiera había que hacer eso, porque la información estaba ahí frente a todos.

Para demostrar lo aberrante del caso, Vilariño ejemplificó cómo funcionaba el sitio haciendo un paralelismo simple y fácil de asimilar:

*"Es como si vos fueses caminando por Diagonal Norte, y pases por la puerta del Registro Nacional de las Personas (ReNaPer). El edificio en vez de tener paredes de piedra, son todas de vidrio. Y sobre el vidrio, mirando hacia afuera, están pegados todos los expedientes de todos los ciudadanos. Entonces vos podés pasar caminando por ahí y ver lo que quieras. No sólo eso, si buscás un DNI encontrás exactamente la ficha de ciudadano que vos querés. Así fue esto, pero de manera digital."*

Si bien casos así también se ven en empresas privadas, dónde puedo elegir tranzar con el servicio que me están dando a cambio de mis datos, en éste caso es mucho más preocupante: son datos que se extraen de manera coercitiva, no se puede decidir no aportar esta información a la AFIP, porque la ley así lo obliga. Acá el problema es que no se están cuidando datos que son privados, problemática que no es nueva para los sitios del Estado, no hay responsabilidad.

El sitio vulnerable ya fue dado de baja. Ni se arregló, ni se modificó, solamente se "apagó" y el Estado aún no comentó nada al respecto a pesar de las claras demandas.