

## Pueden robar tus datos usando los perfiles de autocompletado

Las características de autocompletado del Navegador pueden usarse para robo de datos personales en campañas de *phishing*

La función de Autocompletar, cuando está habilitada, permite recordar usuario y clave u otros datos como teléfono, dirección, mail, etc.

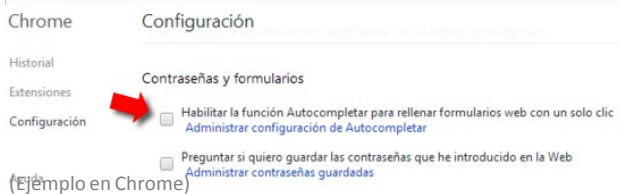
Pero esta característica puede resultar peligrosa, ya que permite que terceros accedan a estos datos sin que nos demos cuenta. Para

hacerlo se usa una web creada para la ocasión (*phishing*) y basta con invitar a los usuarios a que rellenen su nombre y su dirección de mail. A partir de ahí, el *hack* se aprovecha de que, al introducir la primera letra de su nombre, el usuario usará la sugerencia de autocompletado tan rápido como aparezca.

Así, los datos se rellenan automáticamente, y aunque la persona que los ha introducido pueda pensar que el navegador estaba, por ejemplo, introduciendo su dirección de correo electrónico por él, en realidad estaba almacenando sus datos personales. No solo la dirección electrónica, sino que también se puede conseguir el domicilio postal, el número de teléfono y otros detalles.

Estos campos pueden estar ocultos, y por consiguiente el usuario no advierte que está relleno esa información.

Por el momento, la sugerencia es deshabilitar la función de Autocompletar.



(Ejemplo en Chrome)



## ¡Vienen por mi Apple-ID!



Hay que tener cuidado con los supuestos avisos de los fabricantes.

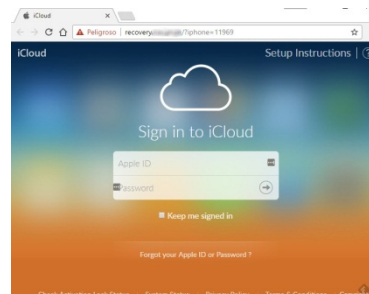
Esta es la crónica en primera persona de un Consultor en Seguridad Informática.

*Hace unos días, Apple Inc. se puso en contacto conmigo. Eligieron una forma muy interesante: un SMS en español. Y lo mejor es que, evidentemente, deben tener líneas locales porque el número del cual me escribieron tenía la característica de la ciudad donde vivo, Buenos Aires.*



*Cuando recibí el mensaje, me sucedieron dos cosas: primero me emocioné, porque a mí efectivamente me habían robado el celular en noviembre de 2016, pero después dudé. Todo era raro.*

*Decidí esperar, no entrar al enlace y hacerlo desde uno de los equipos de nuestro Laboratorio de Investigación de malware, por las dudas. Al hacerlo, Google Chrome directamente me avisó que ese sitio **podía ser peligroso**.*



*El resultado: una réplica de la pantalla de ingreso a la nube de Apple. Un truco para llevarse mis credenciales. Probé ingresando datos erróneos y me derivó a otra falsa página: ¡confirmada la maniobra!*

