COMUNICADO DE PRENSA

Viernes, 5 de febrero de 2021

El Departamento de Justicia y su Unidad Investigativa de Crímenes Cibernéticos alertan sobre esquemas de fraude a través de ATH Móvil, WhatsApp y Facebook

(San Juan, Puerto Rico) – El Secretario de Justicia Domingo Emanuelli Hernández, la Jefa de Fiscales Melissa Vázquez Sandoval junto al Director de la Unidad Investigativa de Crímenes Cibernéticos Gilberto Gierbolini Merino alertan a la ciudadanía sobre un esquema de fraude que está sucediendo mediante el servicio de mensajes WhatsApp, Facebook y la aplicación de ATH Móvil.

En las pasadas semanas se ha visto un aumento de quejas en las redes sociales en la que alegan que personas están robando su identidad, éstos conocidos como “hackers”, utilizando mayormente las cuentas de WhatsApp y Facebook. Luego que estos hackers logran el acceso a sus cuentas, comienzan a escribir mensajes a sus contactos solicitándoles dinero de emergencia y alegando que se los devolverán al día siguiente. Cuando a la persona le indica que le va a enviar el dinero a su conocido, el hacker le envía un mensaje con un número de teléfono distinto para que le pase el dinero por ATH Móvil.

Hay dos tipos de víctimas en este esquema, al que le roban la cuenta (víctima 1) y al que le piden dinero (victima 2). Víctima 1 recibe un mensaje de un conocido, al que ya le hackearon el WhatsApp o el Facebook, indicándole que está restableciendo el teléfono y que el código no le llega, le pregunta que si puede poner para que el código le llegue a víctima 1 para que cuando le reciba el código, víctima 1 se lo dé al hacker. (ver foto 1)

(Continua en la próxima página)

COMUNICADO DE PRENSA

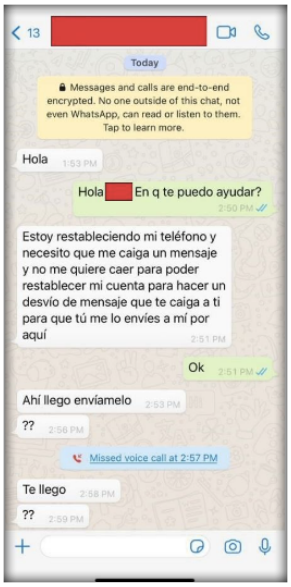

Foto 1: Mensaje solicitando pin de acceso de WhatsApp para tomar control de la cuenta.

Una vez el mensaje de WhatsApp con el pin le llega a la víctima 1, esta se lo brinda al hacker y es así como el hacker le puede tomar el control de la cuenta. (ver foto 2)

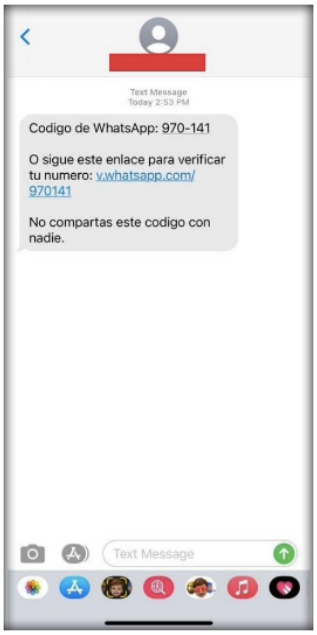

Foto 2: Mensaje de texto que le llega a la victima 1 de la Aplicación de WhatsaApp.

(Continua en la próxima página)

Una vez el hacker tiene el control de la víctima 1, comienza a escribirle a los contactos solicitándole dinero. En esta etapa el hacker le comienza a escribir a la víctima 2, por ejemplo, que ya paso el máximo por ATH Móvil y necesita que le preste dinero y que se los pagará. Es ahí cuando le brinda otro número de teléfono para que le pase el dinero por la aplicación de ATH Movil. (Ver foto 3)

Foto 3: Mensaje de usuario de Facebook donde alega que le trataron de estafar.

Una vez la víctima envía ese código, está autorizando al delincuente a que tome control sobre su cuenta.

Por otro lado, en este momento es necesario alertar a la ciudadanía y que tengan en cuenta:

- Las personas que hayan sido víctima de este esquema deben acudir al cuartel más cercano para realizar la querella correspondiente e iniciar la investigación criminal.
- Estar siempre alerta y consciente que cuando una compañía le envíe código de celular a su equipo, no lo compartan con nadie.
- Asegurarse cuando van a enviar dinero a través de la aplicación ATH Móvil que la persona que lo va a recibir tenga acceso al mismo.

(Continua en la próxima página)

El titular de Justicia sostuvo que “es importante que la ciudadanía conozca de este tipo fraudes, que no den su información personal a nadie que no conozcan y no envíen dinero por ATH Móvil a ningún desconocido. Igualmente, no deben de enviar ningún código de acceso a nadie. También se les recomienda activar la opción de doble verificación de WhatsApp y de Facebook, para así evitar que le roben el acceso a sus cuentas”.

###