Otra vez la estafa por WhatsApp: hackean cuentas con el logo de la app Cuidar y un “cuento” sobre vacunas

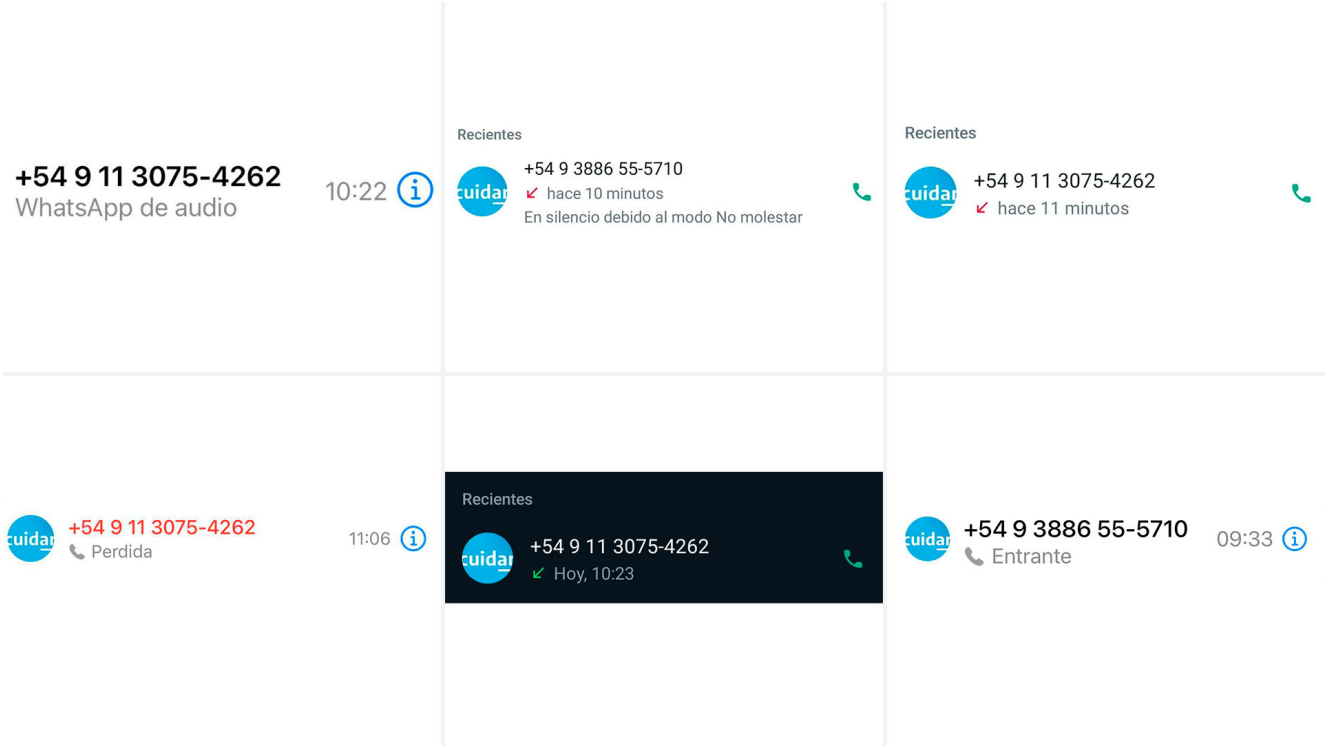
24/05/2023

“Recién me llamaron por Whatsapp de ‘**Cuidar**’, diciéndome que me tenían que mandar el certificado nuevo de las vacunas, les seguí la corriente porque sabía que era una estafa”, contó un contacto en un grupo de trabajo y de inmediato casi una decena más dijo que le había pasado lo mismo. La novedad de esta vieja modalidad de intento de estafa es que la llamada tiene el logo de esa aplicación, tan necesaria y usada cuando comenzó la campaña de vacunación contra el coronavirus.

Es justamente esa la pata que los estafadores encontraron esta vez para acudir a los llamados que buscaban preocupar a los

receptores: “Hablamos desde el **Ministerio de Salud** para saber si completó la cuarta y quinta dosis de la vacuna contra la COVID”, dijo una persona que se presentó como médico en otra llamada.

¿Qué buscan? Hacer creer a la persona que necesitará un nuevo carnet de vacunas, que claramente no tiene, y la convencen para que lo acepte, para esto le piden datos personales y luego inicia el intercambio de números que ellos usarán.



Las llamadas que recibieron integrantes de un mismo grupo de WhatsApp

“El ciberdelincuente ingresa el número telefónico al que la cuenta de WhatsApp está asociada en un dispositivo nuevo y envía el código de verificación a la línea asociada a esa cuenta, ya sea por SMS o por llamada telefónica, claro que sin que el dueño de la cuenta lo sepa. Si se trata de una mensaje de texto, los delincuentes suelen enviar un mensaje por WhatsApp o llamar por teléfono al dueño de la cuenta y fingir ser de una empresa o de algún organismo oficial, como el Ministerio de Salud. En medio del engaño, el estafador generalmente le pide al usuario ese código que llegó por SMS

con alguna excusa, como ‘validar la identidad’, para ‘facilitar’ el trámite”, explica **Emiliano Piscitelli**, especialista en Seguridad Informática.

“El objetivo de los ciberdelincuentes somos todos”, aseguraron en octubre de 2020 los expertos en ciber seguridad durante una conferencia virtual en la que presentaron el estudio “COVID-19 – CIBERPANDEMIA: la otra cara de la crisis sanitaria”, según el cual –afirmaban– la industria del ciberdelito creció exponencialmente desde la llegada del virus.

Cómo estafan por WhatsApp

Cuando se instala por primera vez la app WhatsApp en un celular o si se la reinstala en otro dispositivo, la misma App envía un código de verificación para hacerlo efectivo. Este paso es justamente el que utilizan en mayor medida los estafadores para instalar una cuenta de un usuario en otro dispositivo y así robar todos sus contactos.

Aunque para la posible víctima **la modalidad es nueva, ésta ya tiene unos años y lo único que varía es la “excusa”** que encuentran para llegar al usuario al que buscan robar la identidad por medio de su cuenta. Una vez que se apoderan, van por todos sus contactos con el objetivo de engañarlos y obtener dinero.

Fue justamente durante la pandemia, en plena campaña de vacunación contra el coronavirus, que comenzaron a circular las estafas en esta app para conseguir este código con la excusa de confirmar o empadronar un turno para la vacuna.

“Puede pasar que una persona conocida o no, te diga que por equivocación puso tu número para recuperar su cuenta de WhatsApp, y que si te llegó un SMS, le pases el número y así de simple, en cuestión de minutos, otra persona se apodera de tu cuenta de WhatsApp y de todos nuestros contactos”.

Además, duplican la tarjeta SIM de los teléfonos celulares

engañando de esa manera a las operadoras telefónicas para obtenerlo a nombre de otra persona, lo que hace todavía más fácil la estafa por WhatsApp, ya que el código de verificación llega de manera directa al nuevo dispositivo con la nueva línea.

El único fin que tiene esta modalidad es engañar a la lista de contactos y extraerles dinero. Hay unas tres grandes modalidades de estafa. Una es la de tomar la identidad de la víctima, decirle que habla de un nuevo número y que necesita un préstamo, por ejemplo.

La importancia de la verificación en dos pasos (Freepik)

La verificación en dos pasos

Una de las maneras más efectivas de evitar caer en esta artimaña es “activar la verificación en dos pasos, configurar la privacidad (solo dar visibilidad a contactos o a nadie)”, según el experto.

“Es un número también de 6 dígitos que no hay que compartir con nadie, tiene que ser privado”, dijo sobre la opción que se encuentra en los ajustes de la propia app (los tres puntitos a

la derecha, en Android y abajo en iPhone). Este numero es adicional al otro, por eso son dos pasos. El otro paso es poner un correo para recuperarlo en caso de olvidar ese número. Entonces es este número más el que llega por SMS. Activarlo es una manera de protegerse, pero es importante saber que nadie llamará para pedirles datos personales por teléfono y que en caso de recibir el llamado, no hay que darles nada".

También recomienda que, en caso de ser víctima, se debe hacer la denuncia ante la autoridad judicial correspondiente por delitito informativo y reportar este incidente a support@whatsapp.com con el asunto: "Pérdida/Robo: desactivar mi cuenta".

"No olvidemos que harán estafas con tu cuenta y a tu nombre, por eso es importante denunciar cuando se fue víctima de este tipo de estafa", agrega.

Fuente: Infobae